Nodal lines and surfaces of arithmetic random waves

Maffucci, Riccardo Walter

Awarding institution:
King's College London

KING'S COLLEGE LONDON

School of Natural and Mathematical Sciences

Department of Mathematics

Nodal lines and surfaces of arithmetic random waves

PhD thesis

Candidate: Riccardo Walter Maffucci

Advisor: Dr. Igor Wigman

Second advisor: Prof. Fred Diamond

2017

Abstract

This thesis discusses various aspects of nodal sets of random Gaussian Laplace eigenfunctions ('arithmetic random waves') on the two- and three-dimensional tori. The first problem concerns the number of nodal intersections against a straight line segment in two dimensions. The expected intersections number, against any smooth curve, is universally proportional to the length of the reference curve, times the wavenumber, independent of the geometry. I bounded the variance in the case of a straight line with rational slope. Without assuming rational slope, I proved that the same bound holds unconditionally for a density one sequence of energies, and conditionally for all energies.

The three-dimensional analogue of the first problem is the study of the nodal intersections variance against a straight line segment on the three dimensional torus. I gave a bound for rational lines. For irrational lines, I proved an unconditional result, and a stronger conditional result. I also found a better bound for irrational lines (a_1, a_2, a_3) where a_2/a_1 is rational.

The third problem is work in collaboration with J. Benatar. We studied the area of the nodal set in the three dimensional case. The expected area is proportional to the square root of the eigenvalue. We established an asymptotic formula for the nodal area variance.

The methods involve the theory of random processes, the study of the covariance function and application of Kac-Rice formulas. The problems are closely related to the theory of lattice points on circles and spheres. I proved upper bounds for the number of lattice points on spheres that lie on a thin spherical segment, using Diophantine approximation. Together with J. Benatar, I bounded the number of non-degenerate 4-correlations, and 6-correlations, of lattice points on spheres.

Declaration

This thesis incorporates the following publications:

- [53] Riccardo W. Maffucci, "Nodal intersections of random eigenfunctions on the 2-dimensional torus", Monatsh Math (2017) 183:311-328.
  DOI: 10.1007/s00605-016-1001-2; arXiv: 1603.09646.

- [52] Riccardo W. Maffucci, "Nodal intersections for random waves against a segment on the 3-dimensional torus", Journal of Functional Analysis 272.12 (2017): 5218-5254.
  DOI: 10.1016/j.jfa.2017.02.011; arXiv: 1611.00571.

- [4] Jacques Benatar and Riccardo W. Maffucci, "Random waves on $\mathbb{T}^3$: nodal area variance and lattice point correlations"; to appear in International Mathematics Research Notices.
  DOI: 10.1093/imrn/rnx220; arXiv:1708.07015.

I hereby declare that, except for the explicitly stated collaboration mentioned above, I am the sole author of this thesis.

Acknowledgements

First of all, I would like to deeply thank my supervisor Igor Wigman. This work would not have been possible without his continuous guidance, support, insight, availability, and interest throughout these four years. I am very grateful to Igor also for suggesting the very interesting problems of this thesis, and for suggesting the collaboration with Jacques Benatar.

My PhD was funded by a Graduate Teaching Scholarship (formerly known as Graduate Teaching Assistantship), awarded by the Department of Mathematics, King's College London. I would like to thank the Department, the School of Natural and Mathematical Sciences, and King's College London, for the funding and for being a stimulating workplace for this PhD.

Special thanks to Zeév Rudnick for reading my preprints and for helpful corrections, suggestions, and remarks. Many thanks to my second supervisor Fred Diamond. I would like to thank Jacques Benatar for many helpful discussions and his collaboration in our joint work. Many thanks to Shagnik Das, Fred Diamond, Pär Kurlberg, Domenico Marinucci, Erez Nesharim, Alberto Perelli, and Joshua Zahl for valuable discussions and communications. Many thanks to the examiners Dmitry Belyaev and Yiannis Petridis for helpful corrections.

A big thank-you to my family: my parents, grandparents, Valentina, and Lucia, for supporting me always, especially during the most difficult times. Special thanks for their support to Andrea M., Andrea S., Dimitris, Emilio F., Emilio Z., Enrico, Giacomo, Giulio, Ilaria, Jacques, Marco M., Marco P., Massimo, Mattia, Maurizia, Maurizio, Michele, Roberta, Robin, Ruben, Silvia, Valentina, Victor. Thanks to all academics, co-workers, students, and friends, that have played an important role during these years at King's.

To my family

*"The secret is,
never give up"*

Contents

List of Figures

Chapter 1

Statement of main results

In the present chapter, we state the main findings of this thesis, published in M. [53, 52], and Benatar-M. [4].

1.1 Introduction

Nodal sets of Laplace eigenfunctions

Nodal sets. Let $\mathcal{M}$ be a smooth compact Riemannian manifold of dimension d, and $G : \mathcal{M} \to \mathbb{R}$ be a real-valued function. The *nodal set* of G is the zero-locus

$$\{x \in \mathcal{M} : G(x) = 0\}. \tag{1.1.1}$$

Its study dates back to Hooke's pioneering experiments, and the alternative name 'Chladni Plates' derives from Chladni's work (17th-18th century). Nodal lines are of interest in the study of waves, and have many applications in the physical and natural sciences, such as astrophysics, engineering, the study of sound, of ocean sea waves and of earthquakes.

Laplace eigenfunctions. Let Δ be the Laplace-Beltrami operator, or for short Laplacian, on $\mathcal{M}$. The study of functions G satisfying the Helmholtz differential equation

$$(\Delta + E)G = 0$$

with eigenvalue (also called 'energy' in this context) $E > 0$, especially in the high energy limit $E \to \infty$, is of great importance in the area of PDEs and in physics. It was established by Cheng [18, Theorem 2.2] that, except for a set of lower dimension (i.e., $< d-1$), the nodal sets of Laplace eigenfunctions on $\mathcal{M}$ are smooth manifolds of dimension $d-1$. For $d = 2$, we call (1.1.1) **nodal line**, for $d = 3$, we call it **nodal surface**.

The manifold $\mathcal{M}$ we shall be working with is the d-dimensional standard flat torus

$$\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d,$$

for $d \geq 2$, with special focus on the cases $d = 2, 3$. Here the Laplacian is

$$\Delta = \frac{\partial^2}{\partial x_1^2} + \frac{\partial^2}{\partial x_2^2} + \cdots + \frac{\partial^2}{\partial x_d^2}.$$

Lattice points on spheres. In the setting of the d-dimensional torus, the study of the nodal lines is closely related to the **d squares problem**, as we shall see next. Let

$$S^{(d)} := \{0 < m : \ m = a_1^2 + \cdots + a_d^2, \ a_i \in \mathbb{Z}\} \tag{1.1.2}$$

be the set of nonzero integers expressible as a sum of d perfect squares. For $d \geq 2$, denote $\mathcal{S}^{d-1} \subset \mathbb{R}^d$ the $d-1$-dimensional sphere. Consider the set of all lattice points on the sphere $\sqrt{m}\mathcal{S}^{d-1}$ of radius $\sqrt{m}$,

$$\mathcal{E}_m^{(d)} := \{\mu = (\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(d)}) \in \mathbb{Z}^d : (\mu^{(1)})^2 + (\mu^{(2)})^2 + \cdots + (\mu^{(d)})^2 = m\}.$$

Their cardinality, or equivalently, the number of ways that m may be written as a sum of d perfect squares, will be also denoted

$$\mathcal{N}_m^{(d)} := |\mathcal{E}_m^{(d)}| = r_d(m).$$

In what follows, we shall simply write $\mathcal{E}, \mathcal{N}$, omitting the indices d, m when these are clear from the context.

Lemma 1.1.1. *The Laplace eigenvalues on $\mathbb{T}^d$ are given by the sequence*

$$\{E_m = 4\pi^2 m\}_{m \in S^{(d)}}.$$

Moreover, given the eigenvalue $E = 4\pi^2 m$, the collection of exponentials

$$\{e^{2\pi i \langle \mu, x \rangle}\}_{\mu \in \mathcal{E}_m}$$

is a basis for the eigenspace. Therefore, all the (complex-valued) eigenfunctions corresponding to the eigenvalue $4\pi^2 m$ have the expression

$$G(x) = \sum_{\mu \in \mathcal{E}_m} g_\mu e^{2\pi i \langle \mu, x \rangle}, \tag{1.1.3}$$

with g_μ Fourier coefficients. It follows that the dimension of the eigenspace is the number of ways $r_d(m)$ that m may be written as a sum of d perfect squares.

The proof and further background are given in section 2.3.

Arithmetic random waves

The eigenvalue multiplicities allow us to work with an ensemble of **random Gaussian Laplace toral eigenfunctions** ('arithmetic random waves') first introduced in 2007 by Oravecz, Rudnick and Wigman [54]:

$$F_m^{(d)}(x) = \frac{1}{\sqrt{\mathcal{N}_m^{(d)}}} \sum_{\mu \in \mathcal{E}_m^{(d)}} a_\mu e^{2\pi i \langle \mu, x \rangle}, \qquad x \in \mathbb{T}^d, \tag{1.1.4}$$

where a_μ are complex standard Gaussian random variables [1] (i.e., $\mathbb{E}[a_\mu] = 0$ and $\mathbb{E}[\|a_\mu\|^2] = 1$). The a_μ are taken to be independent save for the relations $a_{-\mu} = \overline{a_\mu}$, making (1.1.4) real valued. We may equivalently write

$$a_\mu = b_\mu + ic_\mu, \qquad b_\mu, c_\mu \sim N(0, 1/2)$$

[1] Defined on some probability space $(\Omega, \mathcal{F}, \mathbb{P})$, where $\mathbb{E}$ denotes the expectation with respect to $\mathbb{P}$.

and the b_μ, c_μ are independent save for $b_{-\mu} = b_\mu$ and $c_{-\mu} = -c_\mu$.

For a plane wave

$$A(x) = e^{i(\langle \eta, x \rangle + \psi)}$$

we call η the *direction of propagation* and ψ the *phase*. The terminology 'arithmetic random waves' comes from Berry's isotropic monochromatic random waves [5], that propagate uniformly on the circle. The term 'arithmetic' emphasises the fact that the waves (1.1.4) propagate only from rational points on $\mathcal{S}^{d-1}$. Several recent works investigate the fine properties of these random eigenfunctions. In the next section, we will start formulating the problems studied in this thesis, concerning the nodal sets of Laplace eigenfunctions. It is natural to study these problems for 'typical' eigenfunctions, i.e., the ensemble (1.1.4) (also see sections 1.2, 1.3 and 1.4, and the discussions [47, section 1.1], [62, section 1.2]).

Notation. The letters

$$\mu, \mu', \mu'', \mu_1, \mu_2, \ldots$$

will be reserved for elements of the lattice point set $\mathcal{E}_m^{(d)}$. The coordinates of $\mu_5 \in \mathcal{E}_m^{(d)}$, for instance, will be written as

$$\mu_5 = (\mu_5^{(1)}, \mu_5^{(2)}, \ldots, \mu_5^{(d)}).$$

We will use the expression

$$\langle x, y \rangle$$

for the inner product of two vectors x and y.

For two positive functions $f(k), g(k)$, the expression

$$f \sim g$$

means that the ratio of the two sides converges to 1 as k tends to a limit. We write interchangeably

$$f = O(g) \qquad \text{or} \qquad f \ll g$$

(respectively Landau's and Vinogradov's notation) if one has $|f(k)| \leq c|g(k)|$ for some $c > 0$ as k tends to a limit. When c depends on a parameter t, we write $f \ll_t g$. The notation

$$f \asymp g$$

means $g \ll f \ll g$. We write $f = o(g)$ if the ratio f/g converges to 0.

Outline of the thesis. In the rest of the present chapter, we will formulate the three main problems studied in this thesis, together with our main results. The theorems stated in sections 1.2, 1.3 and 1.4 shall be proven in chapters 3, 4 and 5 respectively. In chapter 2, we shall introduce the necessary background for these proofs, coming from a few areas of mathematics. In the appendix, we will prove auxiliary results and perform necessary computations.

1.2 Nodal intersections on the 2-dimensional torus

Asymptotic density of a sequence

We begin by introducing a concept that is key to understanding a few of the statements to follow.

Definition 1.2.1. Let $A' \subseteq A \subseteq \mathbb{Z}$. We say A' has *asymptotic density* l, $0 \leq l \leq 1$ in A if

$$l = \lim_{X\to\infty} \frac{|\{n \in A' : n \leq X\}|}{|\{n \in A : n \leq X\}|}. \tag{1.2.1}$$

For instance, inside the set of the integers, the odd numbers have density $l = \frac{1}{2}$, the primes have density $l = 0$ and the perfect squares have density $l = 0$. We use the term 'generic' for a density one sequence, and the term 'thin' for a density zero sequence.

Formulation of the problem and prior work

Nodal intersections. Several recent works (e.g. [67, 16, 29]) studied the number of intersections between the nodal lines $\mathcal{L}$ of eigenfunctions and a fixed reference curve (*nodal intersections* on 'general' surfaces Σ). This quantity yields information on the geometry of the nodal lines, and in some situations [34] gives lower bounds on the number of nodal domains (i.e., connected components of $\Sigma \setminus \mathcal{L}$). It is expected that in many situations, the nodal intersections number obeys the bound $\ll \sqrt{E}$, where $E > 0$ is the eigenvalue.

The setting. Let $d = 2$ and fix a smooth reference curve $\mathcal{C} \subset \mathbb{T}^2$, of length L. We consider the intersection of the nodal set of the Laplace eigenfunction G,

$$\{x \in \mathbb{T}^2 : G(x) = 0\}, \tag{1.2.2}$$

with $\mathcal{C}$ and count the number of **nodal intersections**

$$|\{x \in \mathbb{T}^2 : G(x) = 0\} \cap \mathcal{C}|, \tag{1.2.3}$$

as $m \to \infty$. Bourgain-Rudnick showed that, if $\mathcal{C} \subset \mathbb{T}^2$ is not a segment of a closed geodesic, then it is not contained in the nodal line (1.2.2) for eigenvalue sufficiently big [9, Theorem 1.1]. Conversely, if $\mathcal{C}$ is a segment of a closed geodesic, then one can construct a sequence of Laplace eigenvalues with eigenfunctions vanishing on $\mathcal{C}$ [9, section 1]. If $\mathcal{C}$ is a segment of an unbounded geodesic, then no eigenfunction can vanish on it [9, section 1]. Moreover, for curves with nowhere vanishing curvature, one has [10, Theorems 1.1 and 1.2]

$$\sqrt{m}^{1-o(1)} \ll |\{x \in \mathbb{T}^2 : G(x) = 0\} \cap \mathcal{C}| \ll \sqrt{m}. \tag{1.2.4}$$

The lower bound in (1.2.4) was strengthened [11] to $\gg \sqrt{m}$ (and is thus optimal up to a constant) conditionally on a number-theoretic conjecture of Cilleruelo-Granville (Conjecture 2.2.7 in section 2.2.2), known to hold for a density one sequence of eigenvalues.

We recall that

$$\mathcal{E} = \{\mu \in \mathbb{Z}^2 : \|\mu\|^2 = m\}$$

is the set of lattice points lying on the circle of radius $\sqrt{m}$, and $\mathcal{N} = |\mathcal{E}|$ is their number. Let us now consider the arithmetic random waves (1.1.4) on $\mathbb{T}^2$,

$$F^{(2)}(x) = \frac{1}{\sqrt{\mathcal{N}^{(2)}}} \sum_{(\mu^{(1)},\mu^{(2)})\in\mathcal{E}} a_\mu e^{2\pi i\langle\mu,x\rangle}, \tag{1.2.5}$$

and investigate the *distribution* of the nodal intersections number

$$\mathcal{Z} = \mathcal{Z}_m^{(2)}(F) := |\{x \in \mathbb{T}^2 : F(x) = 0\} \cap \mathcal{C}| \tag{1.2.6}$$

against a smooth toral curve $\mathcal{C}$, as $m \to \infty$ [2]. Let us compare the deterministic and random settings: in the former, the results of Bourgain-Rudnick [9, 10, 11] hold for a density one sequence of *eigenvalues*, for all the corresponding eigenfunctions; in the latter, we are looking for results for all eigenvalues, and 'typical' eigenfunctions.

The set of energies (1.1.2) on $\mathbb{T}^2$ is $\{E_m = 4\pi^2 m\}_{m\in S^{(2)}}$, where

$$S^{(2)} := \{0 < m : \ m = a_1^2 + a_2^2, \ a_1, a_2 \in \mathbb{Z}\}. \tag{1.2.7}$$

We have the following well-known fact.

Proposition 1.2.2 ([38, §16.9])**.** *Let $m \in \mathbb{N}$, with prime decomposition given by*

$$m = p_1^{\alpha_1} \cdots p_h^{\alpha_h} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l} \cdot 2^\nu,$$

where each $p_i \equiv 1 \pmod 4$ and each $q_i \equiv 3 \pmod 4$.

1. *We have*

$$m \in S^{(2)} \Leftrightarrow 2 \mid \beta_i \quad \textit{for all } 1 \le i \le l.$$

[2]The index 2 in $\mathcal{Z}_m^{(2)}(F)$ is to distinguish from the 3-dimensional analogue of this problem (see section 1.3).

2. For $m \in S^{(2)}$, we have

$$\mathcal{N}_m^{(2)} = 4\prod_{i=1}^{h}(\alpha_i + 1).$$

The proof of Proposition 1.2.2 may be found in section 2.2.2; the key ingredient in this proof is the fact that the ring of Gaussian integers $\mathbb{Z}[i]$ is a unique factorisation domain (UFD). As $m \to \infty$, the number of lattice points on $\sqrt{m}\mathcal{S}^1$ satisfies [38, Theorems 337 and 338]

$$\mathcal{N}_m \ll m^{\epsilon} \qquad \forall \epsilon > 0, \tag{1.2.8}$$

and $\mathcal{N}$ is not bounded by any power of $\log m$. We have $\mathcal{N}_p = 8$ for all primes $p \equiv 1 \pmod 4$; nonetheless, $\mathcal{N} \to \infty$ for a density one sequence of energy levels. The set $\mathcal{E}$ induces a discrete probability measure τ_m on the unit circle $\mathcal{S}^1 \subset \mathbb{C}$ as follows. We denote δ_x the Dirac delta measure supported at x, and define

$$\tau_m := \frac{1}{\mathcal{N}_m}\sum_{\mu\in\mathcal{E}}\delta_{\frac{\mu}{\sqrt{m}}}. \tag{1.2.9}$$

The lattice points on circles are equidistributed along generic subsequences $\{m_k\}_k \subset S^{(2)}$ [30, 31], meaning that, for a density one sequence of energy levels, τ_{m_k} converges weak-* [3] to the uniform measure on the unit circle $d\theta/2\pi$:

$$\tau_{m_k} \Rightarrow \frac{d\theta}{2\pi}. \tag{1.2.10}$$

For further background on lattice points on circles, see section 2.2.2.

Prior work. Rudnick-Wigman [61] and subsequently Rossi-Wigman [59] investigated the number of nodal intersections $\mathcal{Z}$ (1.2.6) of arithmetic random

[3]The statement $\nu_i \Rightarrow \nu$ means that, for every smooth bounded test function g, one has $\int g d\nu_i \to \int g d\nu$.

waves against a reference curve $\mathcal{C} \subset \mathbb{T}^2$. The expected nodal intersections number against smooth curves of length L is [61, Theorem 1.1]

$$\mathbb{E}[\mathcal{Z}] = \sqrt{2m}L. \tag{1.2.11}$$

Moreover, Rudnick-Wigman [61, Theorem 1.2] found the precise asymptotic behaviour of the variance of $\mathcal{Z}$ against smooth curves with *nowhere zero curvature* $\mathcal{C}$ (assuming w.l.o.g. the unit speed parametrisation $\gamma : [0, L] \to \mathcal{C}$):

$$\operatorname{Var}(\mathcal{Z}) = (4B_{\mathcal{C}}(\mathcal{E}) - L^2) \cdot \frac{m}{\mathcal{N}_m} + O\left(\frac{m}{\mathcal{N}_m^{3/2}}\right) \tag{1.2.12}$$

as $m \to \infty$ along a subsequence of $S^{(2)}$ satisfying $\mathcal{N}_m \to \infty$, where

$$B_{\mathcal{C}}(\mathcal{E}) := \int_{\mathcal{C}} \int_{\mathcal{C}} \frac{1}{\mathcal{N}_m} \sum_{\mu \in \mathcal{E}} \left\langle \frac{\mu}{\|\mu\|}, \dot{\gamma}(t_1) \right\rangle^2 \cdot \left\langle \frac{\mu}{\|\mu\|}, \dot{\gamma}(t_2) \right\rangle^2 dt_1 dt_2.$$

For a fixed subsequence $\{m_k\}_k$ satisfying $\mathcal{N}_m \to \infty$, formula (1.2.12) prescribes the asymptotic behaviour of $\operatorname{Var}(\mathcal{Z})$: for instance, assuming the lattice points $\mathcal{E}$ equidistribute (the generic assumption (1.2.10) on the energy levels [30, 31]), one has

$$\operatorname{Var}(\mathcal{Z}) = \left(\int_{\mathcal{C}} \int_{\mathcal{C}} \langle \dot{\gamma}(t_1), \dot{\gamma}(t_2) \rangle^2 dt_1 dt_2 - \frac{L^2}{2}\right) \cdot \frac{m}{\mathcal{N}_m} \cdot (1 + o(1))$$

as $m \to \infty$ s.t. $\mathcal{N} \to \infty$. The asymptotic behaviour (1.2.12) is non-universal, as $B_{\mathcal{C}}(\mathcal{E})$ depends both on $\mathcal{C}$ and on the limiting angular distribution of the lattice points on the circle $\sqrt{m}\mathcal{S}^1$.

A nice consequence of (1.2.11) and (1.2.12) is that the normalised number of nodal intersections $\mathcal{Z}/\mathbb{E}[\mathcal{Z}]$ is a random variable with mean 1 and vanishing variance (as $m \to \infty$ along a sequence such that $\mathcal{N} \to \infty$): therefore, its distribution is asymptotically concentrated at the mean value, i.e., for all $\epsilon > 0$,

$$\lim_{\mathcal{N} \to \infty} \mathbb{P}\left(\left|\frac{\mathcal{Z}(F)}{\sqrt{2m}L} - 1\right| > \epsilon\right) = 0. \tag{1.2.13}$$

The leading coefficient in (1.2.12) is always non-negative and bounded [61, sections 1 and 7]:

$$0 \leq 4B_{\mathcal{C}}(\mathcal{E}) - L^2 \leq L^2,$$

though it might vanish, for instance when $\mathcal{C}$ is a circle, independent of $\mathcal{E}$. Rossi-Wigman [59] investigated the scenario of 'static curves', i.e., those such that $4B_{\mathcal{C}}(\mathcal{E}) - L^2$ vanishes universally. To present their findings, we need some further background.

First, Landau [50, 36] proved that

$$|\{m \in S^{(2)} : m \leq X\}| \sim \text{const} \cdot \frac{X}{\sqrt{\log X}} \tag{1.2.14}$$

(cf. (2.2.5) to follow). Next, we have the following definition.

Definition 1.2.3. We call a sequence $\{m\} \subset S^{(2)}$ a *Bourgain-Rudnick sequence* if one has

$$\min_{\mu \neq \mu' \in \mathcal{E}} \|\mu - \mu'\| > (\sqrt{m})^{1-\epsilon} \tag{1.2.15}$$

for some $0 < \epsilon < 1$.

Bearing in mind (1.2.14), condition (1.2.15) holds for a density one sequence of energies: in fact, a stronger quantitative statement holds.

Lemma 1.2.4 (Bourgain and Rudnick [8, Lemma 5])**.** *Fix $\epsilon > 0$. Then for all but $O(X^{1-\epsilon/3})$ integers $m \leq X$, one has* (1.2.15)*.*

More recently, Granville and Wigman [36, (16)] proved the bound

$$O(X^{1-\epsilon}(\log X)^{1/2})$$

for the number of exceptions to (1.2.15).

Back to nodal intersections, Rossi and Wigman [59], among other things, found that the precise asymptotic behaviour of the nodal intersections variance, for sequences satisfying $\mathcal{N} \to \infty$ and (1.2.15) for some $0 < \epsilon < 1/2$, in the case of static curves is given by [59, Theorem 1.3]

$$\mathrm{Var}(\mathcal{Z}) = (16A_{\mathcal{C}}(\mathcal{E}) - L^2) \cdot \frac{m}{4\mathcal{N}_m^2} \cdot (1 + o(1)), \tag{1.2.16}$$

where

$$A_{\mathcal{C}}(\mathcal{E}) := \int_{\mathcal{C}} \int_{\mathcal{C}} \frac{1}{\mathcal{N}_m^2} \sum_{\mu,\mu' \in \mathcal{E}} \left\langle \frac{\mu}{\|\mu\|}, \dot{\gamma}(t_1) \right\rangle^2 \cdot \left\langle \frac{\mu'}{\|\mu'\|}, \dot{\gamma}(t_1) \right\rangle^2 \cdot \left\langle \frac{\mu}{\|\mu\|}, \dot{\gamma}(t_2) \right\rangle^2 \cdot \left\langle \frac{\mu'}{\|\mu'\|}, \dot{\gamma}(t_2) \right\rangle^2 dt_1 dt_2.$$

Moreover, the leading term in (1.2.16) is bounded away from zero [59, Theorem 1.3]. For instance, assuming $\mathcal{C}$ to be a full circle of total length L, and $\{m\} \subset S^{(2)}$ a sequence satisfying $\mathcal{N} \to \infty$, (1.2.10), and (1.2.15) for some $\epsilon < 1/2$, then one has [59, Example 1.4]

$$\mathrm{Var}(\mathcal{Z}) \sim \frac{L^2}{32} \cdot \frac{m}{\mathcal{N}^2}.$$

A result for rational line segments

In the rest of the present section 1.2, we state the results of our paper [53]. We study the nodal intersections number (1.2.3) of Laplace eigenfunctions G against *straight line segments* $\mathcal{C} \subset \mathbb{T}^2$,

$$\mathcal{C} : \gamma(t) = t(\alpha_1, \alpha_2), \quad 0 \leq t \leq L, \quad \alpha \in \mathbb{R}^2, \quad \|\alpha\| = 1, \tag{1.2.17}$$

the other extreme of the nowhere zero curvature setting. Bourgain-Rudnick's deterministic result (1.2.4) may fail in this case, and indeed the segment $\mathcal{C}$ might be contained in the nodal set of G for arbitrarily high eigenvalue, hence (1.2.3) may be infinite. Let us then consider the ensemble of arithmetic random waves (1.2.5), and investigate the nodal intersections number $\mathcal{Z}$ (1.2.6). Recall that the expectation of $\mathcal{Z}$, for any smooth toral curve, is given by (1.2.11). We will establish upper bounds for the nodal intersections variance.

The nodal intersections $\mathcal{Z}$ are the zeros of the *random process*

$$f(t) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{\mu \in \mathcal{E}} a_\mu e^{2\pi i t \langle \mu, \alpha \rangle},$$

restriction of the random wave F to $\mathcal{C}$ (see section 2.4 for details). Since f is a trigonometric polynomial of degree $\text{const}_{\mathcal{C}} \cdot \sqrt{m}$, it has $\ll \sqrt{m}$ roots unless it vanishes identically. By [3, Theorem 1], the number of zeros of f is finite with probability 1; in particular, this shows that for typical eigenfunctions, $\mathcal{Z}$ is finite. Bearing in mind (1.2.11), it follows that

$$\text{Var}(\mathcal{Z}) = O(m). \tag{1.2.18}$$

Given $\mathcal{C}$ as in (1.2.17), if $\alpha \in \mathbb{R}^2$ satisfies

$$\alpha_2/\alpha_1 \in \mathbb{Q}, \tag{1.2.19}$$

we say that α is a 'rational vector' and $\mathcal{C}$ a 'rational line segment', otherwise we will say that they are 'irrational'.

Theorem 1.2.5 (M. [53, Theorem 1.1])**.** *Let $\mathcal{C} \subset \mathbb{T}^2$ be a length L rational line segment, and $\{m\} \subset S^{(2)}$ a sequence such that $\mathcal{N} \to \infty$. Then*

$$Var(\mathcal{Z}) = O\left(\frac{m}{\mathcal{N}}\right), \tag{1.2.20}$$

the involved constant depending on $\mathcal{C}$ only.

The proof of Theorem 1.2.5 will be given is section 3.3. The bound (1.2.20) is clearly stronger than the trivial bound (1.2.18); (1.2.20) is of the same order of magnitude as the leading term in (1.2.12) for the case of nowhere zero curvature curves, though we were not able to show the lower bound.

A result for irrational line segments

Without the assumption that $\mathcal{C}$ is a rational line, we may prove the following result unconditionally.

Theorem 1.2.6 (M. [53, Theorem 1.2])**.** *Let $\mathcal{C}$ be a segment on the torus, and $\{m\} \subset S^{(2)}$ a sequence such that $\mathcal{N} \to \infty$. Then*

$$Var(\mathcal{Z}) = O\left(m\left(\frac{\log m}{\mathcal{N}}\right)^{4/5}\right). \tag{1.2.21}$$

The proof of Theorem 1.2.6 will be given is section 3.4. The upper bound (1.2.21) is weaker than (1.2.20). It is stronger than the trivial bound (1.2.18) for all sequences $\{m\} \subset S^{(2)}$ satisfying

$$\log m = o(\mathcal{N}). \tag{1.2.22}$$

For such sequences, in particular (1.2.13) holds.

Examples. We give two examples of sequences satisfying (1.2.22). First, consider an increasing product of distinct primes

$$m_k = \prod_{\substack{p \le k \\ p \equiv 1 \ (4)}} p. \tag{1.2.23}$$

We write

$$\log m_k = \log \prod_{\substack{p \le k \\ p \equiv 1 \mod 4}} p = \sum_{\substack{p \le k \\ p \equiv 1 \mod 4}} \log p \le \theta(k),$$

where

$$\theta(k) := \sum_{\text{primes } p \le k} \log p$$

is Chebychev's function. By the Prime Number Theorem,

$$\theta(k) \sim k,$$

so that

$$\log m_k \ll k. \tag{1.2.24}$$

On the other hand, by Proposition 1.2.2, we have

$$\mathcal{N}_m = 4\prod_i(\alpha_i+1) = 4 \prod_{\substack{p\le k \\ p\equiv 1 \mod 4}} 2 = 2^{\pi(k,4,1)+2}, \tag{1.2.25}$$

where $\pi(k,4,1) = |\{\text{primes } p \le k : p \equiv 1 \mod 4\}|$. By Dirichlet's theorem on primes in arithmetic progressions,

$$\pi(k,4,1) \sim \frac{1}{2}\frac{k}{\log k},$$

so that in particular $\pi(k,4,1) > c\cdot k/\log k$ for some $c>0$ and sufficiently big k. Inserting this into (1.2.25) yields

$$\log_2(\mathcal{N}_m) = \pi(k,4,1)+2 > c\cdot\frac{k}{\log k}$$

hence

$$\mathcal{N}_m > (2^c)^{\frac{k}{\log k}} \tag{1.2.26}$$

for some $c>0$ and sufficiently big k. Combining the estimates (1.2.24) and (1.2.26), we obtain that (1.2.22) holds for the sequence (1.2.23).

Next, consider the increasing product of any bounded number of primes (at least two of them), for instance

$$m_k = (5\cdot 13)^k.$$

In general, we write the prime factorisation

$$m_k = p_1^{\alpha_1(k)}\cdots p_h^{\alpha_h(k)}\cdot q_1^{2\beta_1}\cdots q_l^{2\beta_l}2^{\nu},$$

where each $p_i\equiv 1 \pmod 4$, each $q_i \equiv 3 \pmod 4$, and the p_i, q_j, β_j, h, l and ν are fixed as $k\to\infty$. We order the factors of m so that

$$\alpha_1(k) \ll \alpha_2(k) \ll \cdots \ll \alpha_h(k)$$

for large k. Then, on one hand,

$$\log m_k = \alpha_1\log p_1 + \cdots + \alpha_h \log p_h + 2\beta_1\log q_1 + \cdots + 2\beta_l \log q_l + \nu\log 2 \asymp \alpha_h(k)$$

and on the other hand, by Proposition 1.2.2,

$$\mathcal{N}_m = 4\prod_{i=1}^{h}(\alpha_i + 1) \asymp \prod_{i=1}^{h}\alpha_i(k)$$

hence we get $\log m = o(\mathcal{N}_m)$ for our sequence provided that at least two distinct $\alpha_i(k) \to \infty$ as $k \to \infty$.

A stronger conditional bound

We may improve the bound (1.2.21) of Theorem 1.2.6 conditionally on a conjecture on lattice points on short arcs. Consider a circle of radius $\sqrt{m}$: in light of (1.2.8), one would expect short arcs of the circle to contain a bounded number of lattice points. Indeed, it was proven by Jarnik [45] that on every arc of length $< (\sqrt{m})^{1/3}$ there are at most 2 lattice points. Theorem 1.2.8 below is conditional on a weaker version of a conjecture by Cilleruelo and Granville (Conjecture 2.2.7 in section 2.2.2; see also [22, 21]).

Conjecture 1.2.7. *There exists $\epsilon > 0$ such that on a circle of radius $\sqrt{m}$, on every arc of length $(\sqrt{m})^{1/2+\epsilon}$ there are $O(1)$ lattice points.*

The following will be proven in section 3.4.

Theorem 1.2.8 (M. [53, Theorem 1.4])**.** *Assume Conjecture 1.2.7. Let $\mathcal{C}$ be a segment on the torus, and $\{m\} \subset S^{(2)}$ a sequence such that $\mathcal{N} \to \infty$. Then*

$$Var(\mathcal{Z}) = O\left(\frac{m}{\mathcal{N}}\right).$$

A generic bound

Furthermore, we may improve the bound (1.2.21) of Theorem 1.2.6 unconditionally for a density one sequence of energy levels.

Theorem 1.2.9 (M. [53, Theorem 1.5])**.** *Let $\mathcal{C}$ be a segment on the torus, and $\{m\} \subset S^{(2)}$ a sequence such that $\mathcal{N} \to \infty$ and*

$$\min_{\mu \neq \mu' \in \mathcal{E}_m} \|\mu - \mu'\| > (\sqrt{m})^{1-\epsilon}$$

for some $0 < \epsilon < 1/2$ and sufficiently big m. Then

$$Var(\mathcal{Z}) = O\left(\frac{m}{\mathcal{N}}\right).$$

The proof of Theorem 1.2.9 will be given in section 3.4. Thanks to Lemma 1.2.4, the assumptions of Theorem 1.2.9 hold for a density one sequence of energy levels.

1.3 Nodal intersections on the 3-dimensional torus

Formulation of the problem and prior work

The setting. In dimension $d = 3$, let $\mathcal{C} \subset \mathbb{T}^3$ be a fixed smooth reference curve. For Laplace eigenfunctions G of eigenvalue $E = 4\pi^2 m$, we consider the intersection of the nodal set

$$\{x \in \mathbb{T}^3 : G(x) = 0\} \tag{1.3.1}$$

with $\mathcal{C}$, and count the number of **nodal intersections**

$$|\{x \in \mathbb{T}^3 : G(x) = 0\} \cap \mathcal{C}| \tag{1.3.2}$$

as $m \to \infty$.

As opposed to the two-dimensional analogue (section 1.2), one cannot expect to have any deterministic lower or upper bounds for the number of nodal intersections (1.3.2). Indeed, Rudnick-Wigman-Yesha [62, Examples 1.1, 1.2] constructed sequences of eigenfunctions G and curves $\mathcal{C}$, where $\mathcal{C}$ is contained in the nodal set for arbitrarily high energy, and planar curves with no nodal intersections at all, m arbitrarily large. In the case of planar curves, one considers [62, Example 1.1] the sequence of eigenfunctions $\{G_k\}_{k\geq 1}$,

$$G_k(x_1, x_2, x_3) = \sin(2\pi k x_1),$$

of eigenvalue $E = 4\pi^2 k^2$, with nodal surface given by the planes

$$\{x \in \mathbb{T}^3 : x_1 \in \mathbb{Z}/2k\} :$$

any curve lying on the plane $\{x : x_1 = 0\}$ is contained in the nodal surface for every m, while curves lying e.g. on the plane $\{x : x_1 = 1/2\pi\}$ have empty intersection with the nodal surface for every m.

Let us then consider the arithmetic random waves (1.1.4) on $\mathbb{T}^3$,

$$F^{(3)}(x) = \frac{1}{\mathcal{N}^{(3)}} \sum_{(\mu^{(1)},\mu^{(2)},\mu^{(3)})\in\mathcal{E}} a_\mu e^{2\pi i\langle\mu,x\rangle}, \tag{1.3.3}$$

and investigate the distribution of nodal intersections against $\mathcal{C}$,

$$\mathcal{Z} = \mathcal{Z}_m^{(3)}(F) := |\{x \in \mathbb{T}^3 : F(x) = 0\} \cap \mathcal{C}|, \tag{1.3.4}$$

as $m \to \infty$.

The set of energies is $\{E_m = 4\pi^2 m\}_{m\in S^{(3)}}$, where

$$S^{(3)} := \{0 < m : \ m = a_1^2 + a_2^2 + a_3^2, \ a_1, a_2, a_3 \in \mathbb{Z}\}.$$

An integer m is representable as a sum of three squares if and only if $m \neq 4^l(8k + 7)$, for k, l non-negative integers [38, 24]. Under the assumption $m \not\equiv 0, 4, 7 \pmod 8$, one has

$$(\sqrt{m})^{1-\epsilon} \ll \mathcal{N} \ll (\sqrt{m})^{1+\epsilon} \qquad \text{for all } \epsilon > 0 \tag{1.3.5}$$

[12, section 1]. The condition $m \not\equiv 0, 4, 7 \pmod 8$, ensuring $\mathcal{N}_m \to \infty$, is natural [62, section 1.3]: indeed, if $m \equiv 7 \pmod 8$, the set of lattice points $\mathcal{E}_m^{(3)}$ is empty; on the other hand,

$$\mathcal{E}_{4m} = \{2\mu : \mu \in \mathcal{E}_m\}$$

(see e.g. [38, §20]), hence it suffices to consider energies $m \in S^{(3)}$ up to multiples of 4 (see section 2.2.3 for details).

Prior work. Rudnick, Wigman and Yesha [62] computed the expectation of (1.3.4) to be, for any smooth curve $\mathcal{C}$ of length L on $\mathbb{T}^3$,

$$\mathbb{E}[\mathcal{Z}] = L\frac{2}{\sqrt{3}} \cdot \sqrt{m}. \tag{1.3.6}$$

Moreover, they bounded the variance of $\mathcal{Z}$ for curves with nowhere zero curvature, assuming that $\mathcal{C}$ either has nowhere vanishing torsion [4] or is planar [62, Theorem 1.5]:

$$\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{m^\delta}$$

for $m \not\equiv 0, 4, 7 \pmod 8$, where we may take $\delta = 1/3$ in the case of nowhere vanishing torsion, and any $\delta < 1/4$ for planar curves. It follows that for all $\epsilon > 0$, the number of nodal intersections satisfies [62, Theorem 1.4]

$$\lim_{\substack{m\to\infty \\ m\not\equiv 0,4,7 \pmod 8}} \mathbb{P}\left(\left|\frac{\mathcal{Z}(F)}{\sqrt{m}} - \frac{2}{\sqrt{3}}L\right| > \epsilon\right) = 0, \tag{1.3.7}$$

similar to the two-dimensional case (1.2.13).

A result for rational line segments

In the rest of the present section 1.3 we state the results of our paper [52]. As in the two-dimensional setting, our purpose is to investigate the nodal intersections number (1.3.4) for **straight line segments** of length L

$$\mathcal{C} : \gamma(t) = t(\alpha_1, \alpha_2, \alpha_3), \quad 0 \leq t \leq L, \quad \alpha \in \mathbb{R}^3, \quad \|\alpha\| = 1, \tag{1.3.8}$$

[4]For definitions of curvature and torsion of a curve see e.g. [25, section 1.5].

the other extreme of the nowhere zero curvature setting. Recall that the expected value of $\mathcal{Z}$ is given by (1.3.6). In a moment we will establish upper bounds for the variance, depending on whether the straight line is 'rational', similarly to the 2-dimensional problem. Given $\mathcal{C}$ as in (1.3.8), at least one of the α_i, w.l.o.g. α_1, is non-zero: we call α a *'rational vector'* if

$$\alpha_2/\alpha_1 \in \mathbb{Q} \quad \text{and} \quad \alpha_3/\alpha_1 \in \mathbb{Q};$$

otherwise, we call α an *'irrational vector'*. Accordingly, we say that $\mathcal{C}$ is a *'rational/irrational line segment'*.

Here and elsewhere we will denote

$$R := \sqrt{m},$$

and $R\mathcal{S}^{d-1}$ the $d-1$-dimensional sphere of radius R. We will need the following definition.

Definition 1.3.1 ([10, section 2.3])**.** Let $\kappa_d(R)$ be the maximal number of lattice points in the intersection of $R\mathcal{S}^{d-1} \subset \mathbb{R}^d$ and any hyperplane Π:

$$\kappa_d(R) = \max_{\Pi} \#\{\mu \in \mathbb{Z}^d : \mu \in R\mathcal{S}^{d-1} \cap \Pi\}.$$

We have $\kappa_2(R) \leq 2$ by "Zygmund's trick" [74]. Jarnik (see [45], [10, (2.6)]) found the upper bound

$$\kappa_3(R) \ll R^{\epsilon}, \quad \forall \epsilon > 0. \tag{1.3.9}$$

We denote $\kappa := \kappa_3$, as we will mostly be concerned with κ_d for $d = 3$.

Theorem 1.3.2 (M. [52, Theorem 1.2])**.** *Let the straight line segment $\mathcal{C} \subset \mathbb{T}^3$ be parametrised by $\gamma(t) = t\alpha$, where α is a unit length rational vector. Then the nodal intersections variance has the upper bound*

$$Var\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{\kappa(\sqrt{m})}{\mathcal{N}},$$

the implied constant depending only on α.

The proof of Theorem 1.3.2 may be found in section 4.3.

Results for irrational line segments

For irrational lines we may unconditionally prove the following theorem, distinguishing between irrational lines (1.3.8) satisfying

$$\alpha_2/\alpha_1 \in \mathbb{R} \setminus \mathbb{Q} \quad \text{and} \quad \alpha_3/\alpha_1 \in \mathbb{R} \setminus \mathbb{Q} \tag{1.3.10}$$

and those satisfying

$$\alpha_2/\alpha_1 \in \mathbb{Q} \quad \text{and} \quad \alpha_3/\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}. \tag{1.3.11}$$

Theorem 1.3.3 (M. [52, Theorem 1.3], [52, Theorem 1.4])**.** *Let* $m \not\equiv 0, 4, 7 \pmod 8$ *and* $\mathcal{C} \subset \mathbb{T}^3$ *be an irrational straight line segment, parametrised by* $\gamma(t) = t(\alpha_1, \alpha_2, \alpha_3)$ *with* $\|\alpha\| = 1$*.*

(A). In case (1.3.10) *holds, then we have for all* $\epsilon > 0$

$$Var\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{m^{1/7-\epsilon}}. \tag{1.3.12}$$

(B). In case (1.3.11) *holds, then we have for all* $\epsilon > 0$

$$Var\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{m^{1/5-\epsilon}}. \tag{1.3.13}$$

Parts (A) and (B) of Theorem 1.3.3 will be proven in sections 4.6 and 4.7 respectively. As a consequence of Theorems 1.3.2 and 1.3.3, (1.3.7) is valid for all straight lines.

A stronger conditional result

We may improve the bounds (1.3.12) and (1.3.13) conditionally on a conjecture about lattice points in *spherical caps* (see Definition 4.4.1). Jarnik [45] (see also [9, Theorem 2.1]) proved that, for the sphere $R\mathcal{S}^2$, there is some $C > 0$ such that all lattice points in a cap of radius $< CR^{1/4}$ lie on the same plane. By (1.3.9), it follows that every cap of radius $< CR^{1/4}$ contains $\ll R^{\epsilon}$ lattice points. Theorem 1.3.5 below is conditional on the following conjecture.

Conjecture 1.3.4 (Bourgain and Rudnick [10, section 2.2]). *Let $\chi(R,s)$ be the maximal number of lattice points in a cap of radius s of the sphere $R\mathcal{S}^2$. Then for all $\epsilon > 0$ and $s < R^{1-\delta}$,*

$$\chi(R,s) \ll R^{\epsilon}\left(1+\frac{s^2}{R}\right)$$

as $R \to \infty$.

Theorem 1.3.5 (M. [52, Theorem 1.6]). *Assume Conjecture 1.3.4. Let $m \not\equiv 0,4,7 \pmod 8$ and $\mathcal{C}$ be a straight line segment (rational or irrational) on $\mathbb{T}^3$. Then we have for all $\epsilon > 0$*

$$Var\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{m^{1/4-\epsilon}}.$$

The proof of Theorem 1.3.5 will be given in section 4.8.

Let us compare the results in the present section with those in section 1.2 for nodal intersections against a straight line on the two-dimensional torus. For rational lines, the statement of Theorem 1.3.2 is weaker relatively to the two-dimensional analogue Theorem 1.2.5. For irrational lines, Theorem 1.3.3 prescribes an unconditional bound for all energies $m \in S^{(3)}$, whereas in the two-dimensional setting, an unconditional bound is only given for a *density one sequence* of energies, and a bound for all $m \in S^{(2)}$ is given conditionally (in Theorems 1.2.9 and 1.2.8 respectively). These differences arise because the structure of lattice points on spheres is significantly different from that of lattice points on circles: as a first manifestation of this, compare (1.3.5) and (1.2.8). Further details may be found in section 2.2.

1.4 Nodal area on the 3-dimensional torus

Formulation of the problem and prior work

The setting. Recall that, for a Laplace eigenfunction G on a smooth compact Riemannian manifold $\mathcal{M}$ of dimension d, the nodal set (1.1.1) is a smooth manifold of dimension $d-1$, except for a subset of lower dimension. Consider the $(d-1)$-dimensional **nodal volume** of G,

$$\mathrm{Vol}(\{x \in \mathcal{M} : G(x) = 0\}).$$

A fundamental conjecture of Yau [71, 72] asserts that one has the sharp bounds

$$\sqrt{E} \ll_{\mathcal{M}} \mathrm{Vol}(\{x \in \mathcal{M} : G(x) = 0\}) \ll_{\mathcal{M}} \sqrt{E}, \tag{1.4.1}$$

where E is the eigenvalue of G. This conjecture was established for manifolds $\mathcal{M}$ with a real analytic metric (see Donnelly-Fefferman [26], and Brüning-Gromes [14, 15]), thus in particular it holds for the torus $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$. The lower bound in Yau's conjecture was proven for general smooth $\mathcal{M}$ by Logunov [51].

Prior work. In the setting of arithmetic random waves $F : \mathbb{T}^d \to \mathbb{R}$ (1.1.4), let

$$\mathcal{V} = \mathcal{V}^{(d)} := \mathrm{Vol}(\{x \in \mathbb{T}^d : F(x) = 0\})$$

denote the $(d-1)$-dimensional nodal volume of F. Rudnick and Wigman computed the expected value to be, for $d \geq 1$,

$$\mathbb{E}[\mathcal{V}] = \mathcal{I}_d\sqrt{m}, \qquad \mathcal{I}_d := \sqrt{\frac{4\pi}{d}} \cdot \frac{\Gamma\left(\frac{d+1}{2}\right)}{\Gamma\left(\frac{d}{2}\right)} \tag{1.4.2}$$

[60, Proposition 4.1], consistent to Yau's conjecture (1.4.1). Moreover, Rudnick-Wigman proved the following bound for the variance: for $d \geq 2$,

$$\mathrm{Var}(\mathcal{V}) \ll \frac{m}{\sqrt{\mathcal{N}}} \qquad \text{as } \mathcal{N} \to \infty \tag{1.4.3}$$

[60, Proposition 6.1]. As a consequence, the nodal volume concentrates around its mean as $m, \mathcal{N} \to \infty$ (see [47, section 1.2]).

Rudnick and Wigman [60, section 1] conjectured that the stronger bound

$$\mathrm{Var}(\mathcal{V}) \ll \frac{m}{\mathcal{N}} \tag{1.4.4}$$

should hold. A deep result of Krishnapur, Kurlberg and Wigman [47] is the precise asymptotic behaviour of the variance for $d = 2$ (where the volume is the length of the nodal lines). For any subsequence of energies $\{m_k\}_k \subset S^{(2)}$ such that the multiplicities $\mathcal{N}_{m_k} \to \infty$, it was shown in [47, Theorem 1.1] that

$$\mathrm{Var}(\mathcal{V}^{(2)}) = c_{m_k} \frac{m_k}{\mathcal{N}_{m_k}^2}(1 + o(1)), \tag{1.4.5}$$

where the positive real numbers c_{m_k} depend on the limiting angular distribution of $\mathcal{E}_{m_k}^{(2)}$ - the asymptotics for the variance are *non-universal* (see [47, section 1.2]). Also remarkably, the order of magnitude of (1.4.5) is much smaller than the conjectured (1.4.4), as the terms of order $m/\mathcal{N}$ in the asymptotic expression for the nodal length variance cancel perfectly: this effect was observed by Krishnapur-Kurlberg-Wigman [47, section 1.6], and called *arithmetic Berry cancellation*, after 'Berry's cancellation phenomenon' [5, 70].

In higher dimensions $d > 2$, it was known [69] that the same cancellation should occur, and in particular

$$\mathrm{Var}(\mathcal{V}^{(d)}) \ll m \cdot \mathcal{R}_m^{(d)}(4),$$

where

$$\mathcal{R}_m^{(d)}(\ell) := \int_{\mathbb{T}^d} |r_F^\ell(x)| dx \tag{1.4.6}$$

is the ℓ-th moment of the *covariance function* of F,

$$r_F(x) := \mathbb{E}[F(y) \cdot F(x+y)] = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i \langle \mu, x \rangle},$$

independent of y (further details on r_F will follow in section 2.4.2; also see [47, section 2]).

The nodal area variance asymptotic

In the rest of the present section 1.4, we state the results of our paper [4], joint work with Jacques Benatar. Our main focus is the 3-dimensional torus $\mathbb{T}^3$. We will denote

$$\mathcal{A} := \mathrm{Vol}(\{x \in \mathbb{T}^3 : F(x) = 0\}) = \mathcal{V}^{(3)} \tag{1.4.7}$$

the **nodal area** of F. Recall that the expectation of $\mathcal{A}$ is given by (1.4.2) with $d = 3$,

$$\mathbb{E}[\mathcal{A}] = \frac{4}{\sqrt{3}}\sqrt{m}. \tag{1.4.8}$$

The nodal area variance has the following precise asymptotic.

Theorem 1.4.1 (Benatar, M. [4, Theorem 1.2])**.** *As $m \to \infty$, $m \not\equiv 0, 4, 7 \pmod 8$, we have*

$$Var(\mathcal{A}) = \frac{m}{\mathcal{N}^2} \cdot \left[\frac{32}{375} + O\left(\frac{1}{\mathcal{N}^{1/14-o(1)}}\right)\right].$$

The proof of Theorem 1.4.1 will be given in section 5.1. The 3-dimensional torus exhibits arithmetic Berry cancellation like the 2-dimensional torus (see section 5.5.4 for more details). We also remark that, unlike the 2-dimensional case, the leading order term does not fluctuate: this is because lattice points on spheres are *equidistributed* (see section 2.2.3).

Two theorems on spectral correlations

An arithmetic problem arises naturally in the computation of $\mathrm{Var}(\mathcal{A})$. For $\ell \geq 2$, define the set of *ℓ-correlations of lattice points on spheres*

$$\mathcal{C}_m^{(d)}(\ell) := \left\{(\mu_1, \dots, \mu_\ell) \in {\mathcal{E}_m^{(d)}}^\ell : \sum_{i=1}^{\ell} \mu_i = 0\right\},$$

and the subset of *non-degenerate* correlations

$$\mathcal{X}_m^{(d)}(\ell) := \left\{(\mu_1, \dots, \mu_\ell) \in \mathcal{C}_m^{(d)}(\ell) : \forall \mathcal{H} \subsetneq \{1, \dots, \ell\}, \sum_{i \in \mathcal{H}} \mu_i \neq 0\right\}.$$

We will use the terminology 'ℓ-correlations of lattice points on spheres' and ℓ-*spectral correlations* [47, section 2.3] interchangeably. For ℓ even, the moments (1.4.6) of the covariance function are related to the ℓ-correlations by

$$\mathcal{R}_m^{(d)}(\ell) = \frac{|\mathcal{C}_m^{(d)}(\ell)|}{\mathcal{N}^\ell},$$

as pointed out for instance in [47, section 2.3]. More details on spectral correlations may be found in section 2.2.5.

To prove Theorem 1.4.1, we shall require the following arithmetic formula.

Proposition 1.4.2 (Benatar, M. [4, Proposition 1.4]). *As $m \to \infty$, $m \not\equiv 0, 4, 7 \pmod 8$, we have*

$$Var(\mathcal{A}) = \frac{m}{\mathcal{N}^2} \cdot \left[\frac{32}{375} + O\left(\frac{1}{\mathcal{N}^{1/14-o(1)}} + \frac{|\mathcal{X}_m^{(3)}(4)|}{\mathcal{N}^2} + \frac{|\mathcal{C}_m^{(3)}(6)|}{\mathcal{N}^4}\right)\right].$$

The proof of Proposition 1.4.2 will be given in section 5.5. We are naturally led to the following arithmetic problem: how big are the sets $\mathcal{C}_m^{(d)}(\ell)$ and $\mathcal{X}_m^{(d)}(\ell)$? The following two theorems are the key ingredients for Theorem 1.4.1.

Theorem 1.4.3 (Benatar, M. [4, Theorem 1.6]). *Letting $m \to \infty$, one has the estimate*

$$|\mathcal{X}_m^{(3)}(4)| \ll \mathcal{N}^{7/4+o(1)}.$$

The proof of Theorem 1.4.3 may be found in section 5.3.1.

Theorem 1.4.4 (Benatar, M. [4, Theorem 1.7]). *Letting $m \to \infty$, one has the estimate*

$$|\mathcal{C}_m^{(3)}(6)| \ll \mathcal{N}^{11/3+o(1)}.$$

Theorem 1.4.4 will be proven in section 5.3.2.

Corollary 1.4.5 (Benatar, M. [4, Corollary 1.8]). *For any even length $\ell \geq 8$ one has the bounds*

$$\mathcal{N}^{\ell-3-o(1)} \ll |\mathcal{X}_m^{(3)}(\ell)| \ll \mathcal{N}^{\ell-7/3+o(1)}. \tag{1.4.9}$$

as $m \to \infty$, $m \not\equiv 0, 4, 7 \pmod 8$. The upper bound holds for all $\ell \geq 6$.

Corollary 1.4.5 will be proven in section 5.3.3.

Chapter 2

Background

In the present chapter we introduce concepts and review prior work that will be used in the proof of the main results.

2.1 Results from analytic number theory

Equidistribution

We will mostly be concerned with uniform distribution in the unit circle, though of course any interval may in principal be used.

Definition 2.1.1. We say that a bounded sequence of real numbers $\{c_n\}_{n\geq 1}$ is **equidistributed** $\pmod{2\pi}$ if, for every subinterval $(a,b) \subset [0,2\pi)$, we have

$$\lim_{X\to\infty} \frac{1}{X} \left|\{n \leq X :\ c_n \pmod{2\pi} \in (a,b)\}\right| = \frac{b-a}{2\pi}.$$

We have the following criterion for equidistribution.

Proposition 2.1.2 (Weyl's criterion [48, Theorem 2.1])**.** *A bounded sequence of real numbers* $\{c_n\}_{n\geq 1}$ *is equidistributed* $\pmod{2\pi}$ *if and only if, for every* *non-zero integer k, we have*

$$\lim_{X\to\infty} \frac{1}{X} \sum_{n=1}^{X} e^{ikc_n} = 0.$$

Weyl's law

Let $\mathcal{M}$ be a smooth compact Riemannian manifold of dimension d, and Δ be the Laplacian on $\mathcal{M}$. We define the *spectral counting function* $N(\lambda)$ to be the number of eigenvalues of Δ not exceeding λ, counted with multiplicity. A celebrated theorem of Hörmander asserts that [40, 57, 42, 63]

$$N(\lambda) = C_d \mathrm{vol}(\mathcal{M})\lambda^{d/2} + O(\lambda^{(d-1)/2})$$

for a constant C_d depending on the dimension only. Determining the optimal bound for the error term

$$R(\lambda) := N(\lambda) - C_d \mathrm{vol}(\mathcal{M})\lambda^{d/2}$$

is in general a hard problem. In the case of $\mathcal{M} = \mathbb{T}^2$, it is the classical Gauss circle problem (see section 2.2.2), still far from being solved.

Diophantine approximation

We present the statement and the proof of a result of Dirichlet about the simultaneous approximation of two irrational numbers by rationals. The result easily generalises to any number of irrationals. For a reference, see [10, proof of Lemma 2.5], [38, section 11.12] or [65, section II, Theorem 1A].

Proposition 2.1.3 (Dirichlet)**.** *Given $\zeta_1, \zeta_2 \in \mathbb{R} \setminus \mathbb{Q}$ and an integer $H \geq 1$, there exist $q, p_1, p_2 \in \mathbb{Z}$ so that $1 \leq q \leq H^2$ and*

$$\left|\zeta_1 - \frac{p_1}{q}\right|, \left|\zeta_2 - \frac{p_2}{q}\right| < \frac{1}{qH}.$$

Proof. Denote by $\{x\}$ the fractional part of a real number x (i.e., $\{x\} = x - \lfloor x \rfloor$). Consider the $H^2 + 1$ points

$$(\{0\}, \{0\}), (\{\zeta_1\}, \{\zeta_2\}), (\{2\zeta_1\}, \{2\zeta_2\}), \ldots, \left(\{H^2\zeta_1\}, \{H^2\zeta_2\}\right),$$

belonging to the unit square $[0, 1) \times [0, 1)$. Partition the unit square into H^2 smaller squares

$$\left[i\frac{1}{H}, (i+1)\frac{1}{H}\right) \times \left[j\frac{1}{H}, (j+1)\frac{1}{H}\right),$$

with $0 \leq i, j \leq H - 1$: by the pigeonhole principle, there exists at least one small square containing at least two of the $H^2 + 1$ points. That is to say, there exist $c, d \in \mathbb{Z}$ so that $0 \leq c < d \leq H^2$ and the two points $(\{c\zeta_1\}, \{c\zeta_2\})$ and $(\{d\zeta_1\}, \{d\zeta_2\})$ belong to the same small square; thus $|\{d\zeta_1\} - \{c\zeta_1\}| < 1/H$ and $|\{d\zeta_2\} - \{c\zeta_2\}| < 1/H$. We rewrite

$$|(d-c)\zeta_1 - (\lfloor d\zeta_1 \rfloor - \lfloor c\zeta_1 \rfloor)| < \frac{1}{H}, \qquad |(d-c)\zeta_2 - (\lfloor d\zeta_2 \rfloor - \lfloor c\zeta_2 \rfloor)| < \frac{1}{H}$$

hence there exist integers $q := d - c$, $p_1 := \lfloor d\zeta_1 \rfloor - \lfloor c\zeta_1 \rfloor$ and $p_2 := \lfloor d\zeta_2 \rfloor - \lfloor c\zeta_2 \rfloor$ with $1 \leq q \leq H^2$ and satisfying

$$|q\zeta_1 - p_1|, |q\zeta_2 - p_2| < \frac{1}{H},$$

i.e.,

$$\left|\zeta_1 - \frac{p_1}{q}\right|, \left|\zeta_2 - \frac{p_2}{q}\right| < \frac{1}{qH}.$$

□

Background on lattices

We borrow results and terminology of the present subsection from [66] and [17].

Definition 2.1.4. An n-dimensional *lattice* L (or 'discrete vector group' or 'discrete module') is a discrete subgroup of $\mathbb{R}^n$. Equivalently, it is a subgroup of $\mathbb{R}^n$ not containing vectors of arbitrarily small (positive) length.

The fundamental example is $\mathbb{Z}^n$, called the *integer lattice*. The **rank** r of an n-dimensional lattice L is the maximum number of linearly independent vectors in L; clearly $0 \leq r \leq n$. In case $r = n$, we call L a *full rank lattice.*

There always exists a set $\{x^{(1)}, \ldots, x^{(r)}\}$ of r vectors of L such that every $l \in L$ may be written in a unique way as a linear combination of the $x^{(i)}$ with integer coefficients. Such a set is called a *basis* for L.

Proposition 2.1.5 ([66, Lecture V, §3])**.** *Let $\{x^{(1)}, \ldots, x^{(r)}\}$ be a basis for L. A necessary and sufficient condition that r linearly independent vectors*

$$y^{(1)}, \ldots, y^{(r)}$$

also form a basis for L is that

$$y^{(k)} = \sum_{j=1}^{r} u_{kj} x^{(j)}, \qquad k = 1, \ldots, r, \tag{2.1.1}$$

where $U = \{u_{kj}\}$ is an $r \times r$ matrix with determinant ± 1 and integer entries.

One may rewrite (2.1.1) as $Y = UX$, where X, Y are $r \times n$ matrices with rows given by the $x^{(1)}, \ldots, x^{(r)}$ and $y^{(1)}, \ldots, y^{(r)}$ respectively.

Until the end of the section, suppose all lattices to be full rank. By Proposition 2.1.5, the determinant of the $n \times n$ matrix X associated to the lattice L is independent of the choice of basis: we call this quantity the **determinant of the lattice** and denote it

$$d(L) = |\det(X)| > 0.$$

The determinant has a geometric interpretation: in two dimensions, it equals the area of the parallelogram formed by the two vectors of any basis.

A *sublattice* of L is a lattice $M \subseteq L$. By Proposition 2.1.5, the quantity $d(M)/d(L)$ is independent of the choice of bases for L and M; we call it the *index of M in L* and denote it

$$[L : M] = \frac{d(M)}{d(L)} > 0.$$

Definition 2.1.6. Given a full rank lattice L with basis $\{x^{(1)}, \ldots, x^{(n)}\}$, there exist vectors $y^{(1)}, \ldots, y^{(n)}$ such that $\langle x^{(j)}, y^{(k)} \rangle = \delta_{jk}$ (Kronecker's delta). The lattice L^* with basis the $y^{(1)}, \ldots, y^{(n)}$ is called the **dual lattice** of L.

We have

$$L^* = \{l' \in \mathbb{R}^n : \langle l, l' \rangle \in \mathbb{Z} \text{ for all } l \in L\}.$$

With the notation of Definition 2.1.6, if one calls X the matrix with columns the $x^{(1)}, \ldots, x^{(n)}$, then the matrix with columns the $y^{(1)}, \ldots, y^{(n)}$ is $(X^T)^{-1}$, the inverse of the transpose of X. It follows that

$$d(L^*) = \frac{1}{d(L)}.$$

We have the following straightforward properties of the 'polar' * operator: it is an involution, i.e. for any lattice L, one has $(L^*)^* = L$, and it reverses inclusions, meaning

$$M \subseteq L \Rightarrow L^* \subseteq M^*.$$

On applying to a full rank lattice L a nonsingular linear transformation with matrix C, we get another lattice (denoted CL); if X is the matrix associated to a basis of L, then the corresponding matrix for the lattice CL is $C \cdot X$. We now see that for any n-dimensional full rank lattice L, one has $L = C\mathbb{Z}^n$. The determinant of CL is $d(CL) = |\det(C)| \cdot d(L)$. In the special case of a scalar matrix $C = c \cdot I_n$ (where $c \neq 0$), we denote by cL the transformed lattice, of determinant $d(cL) = |c|^n \cdot d(L)$. Finally, we note that $(cL)^* = \frac{1}{c}L^*$.

2.2 Lattice points on circles and spheres

Preliminary remarks

For $d \geq 2$, denote $\mathcal{S}^{d-1} \subset \mathbb{R}^d$ the $d-1$-dimensional sphere. Consider the set of all lattice points on the sphere $\sqrt{m}\mathcal{S}^{d-1}$ of radius $\sqrt{m}$,

$$\mathcal{E}_m^{(d)} := \{\mu = (\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(d)}) \in \mathbb{Z}^d : (\mu^{(1)})^2 + (\mu^{(2)})^2 + \dots + (\mu^{(d)})^2 = m\}. \tag{2.2.1}$$

Their cardinality $r_d(m)$, the number of ways that m can be written as a sum of d perfect squares, will be also denoted

$$\mathcal{N} = \mathcal{N}_m^{(d)} := |\mathcal{E}_m^{(d)}|.$$

In what follows, we shall omit the indices d, m when these are clear from the context. The structure of $\mathcal{E}$ varies greatly with the dimension; a first manifestation of this is the following classical theorem.

Theorem 2.2.1 (Lagrange, 1770 [38, 24])**.** *Every positive integer is the sum of four squares.*

Note that the analogous statement with fewer squares is false.

Symmetries of the lattice point set. The lattice point set $\mathcal{E}^{(d)}$ is invariant under the group of signed permutations $\mathcal{W}^{(d)}$ [60, section 2.2] consisting of permutation of coordinates and sign-change of coordinates e.g., for $d = 3$,

$$(\mu^{(1)}, \mu^{(2)}, \mu^{(3)}) \to (-\mu^{(1)}, \mu^{(2)}, \mu^{(3)}).$$

Lemma 2.2.2 ([60, Lemma 2.3])**.** *For every subset $\mathcal{O} \subseteq \mathcal{E}$ invariant under $\mathcal{W}^{(d)}$ and for each (j, k) we have*

$$\frac{1}{|\mathcal{O}|} \sum_{\mu \in \mathcal{O}} \mu^{(j)} \mu^{(k)} = \frac{m}{d} \cdot \delta_{j,k}.$$

Moreover, for all $x \in \mathbb{R}^d$, we have

$$\frac{1}{|\mathcal{O}|}\sum_{\mu\in\mathcal{O}}\langle \mu, x\rangle^2 = \frac{m}{d}\cdot \|x\|^2.$$

It follows that, in particular,

$$\sum_{\mu_1,\mu_2\in\mathcal{E}^{(d)}}\langle \mu_1,\mu_2\rangle^2 = \frac{m^2\mathcal{N}^2}{d}. \tag{2.2.2}$$

Lattice points on circles $\sqrt{m}\mathcal{S}^1$

The number of lattice points. In the present section, fix the dimension $d = 2$. The lattice point set is

$$\mathcal{E}^{(2)}_m := \{(\mu^{(1)}, \mu^{(2)}) \in \mathbb{Z}^2 : (\mu^{(1)})^2 + (\mu^{(2)})^2 = m\}. \tag{2.2.3}$$

We present the proof of Proposition 1.2.2 [38, §16.9].

Proof of Proposition 1.2.2. Given $m \in S^{(2)}$, we factor it in the ring of Gaussian integers $\mathbb{Z}[i]$ as

$$\prod p^\alpha \cdot \prod q^\beta \cdot 2^\nu = m = A^2 + B^2 = (A + Bi)(A - Bi),$$

where

$$\begin{cases} A + Bi = \prod(a + bi)^{\alpha_1}(a - bi)^{\alpha_2}\prod q^{\beta_1}(1 + i)^{\nu_1}(1 - i)^{\nu_2} i^t \\ A - Bi = \prod(a + bi)^{\alpha_2}(a - bi)^{\alpha_1}\prod q^{\beta_2}(1 + i)^{\nu_2}(1 - i)^{\nu_1} i^{-t} \end{cases}$$

with

$$t = 0, 1, 2, 3, \quad \nu_1 + \nu_2 = \nu, \quad \alpha_1 + \alpha_2 = \alpha, \quad \beta_1 + \beta_2 = \beta.$$

Since $|A+Bi| = |A-Bi|$, then $\beta_1 = \beta_2$ for all β, which are thus all even. There are 4 possible choices for t, $\nu + 1$ choices for ν_1, ν_2 and $\alpha + 1$ choices for α_1, α_2. The 4 possible values of t correspond to the combinations of signs for A and B; a different α_1 changes the representation $m = A^2 + B^2$ in a non-trivial way. However, changing ν_1 multiplies $A + Bi$ by a power of $\frac{1+i}{1-i} = i$, and this has already been taken into account by choosing t. $\square$

Let us consider the cardinality of $\mathcal{E}^{(2)}$ for large m. As $m \to \infty$ (recall (1.2.8)),

$$\mathcal{N}_m \ll m^{\epsilon} \qquad \forall \epsilon > 0,$$

and moreover $\mathcal{N}$ is not bounded by any power of $\log m$ [38, Theorems 337 and 338]. The behaviour of $r_2(m)$ is 'erratic' [60, section 1], in the sense that it is unbounded, but vanishes for arbitrarily large m. There are also sequences $\{m\}$ along which $r_2(m)$ is constant and non-zero: for instance, $r_2(p) = 8$ for every prime $p \equiv 1 \pmod 4$, and $r_2(2^l) = 4$ for every $l \in \mathbb{N}$.

The set of energies

$$S^{(2)} := \{0 < m : \ m = a_1^2 + a_2^2, \ a_1, a_2 \in \mathbb{Z}\} \tag{2.2.4}$$

is of density 0 in the integers ('most' circles have no lattice points at all): more precisely, Landau [50, 36] proved that

$$|\{m \in S^{(2)} : m \leq X\}| = c_{LR} \cdot \frac{X}{\sqrt{\log X}} \left(1 + O\left(\frac{1}{\log X}\right)\right), \tag{2.2.5}$$

where

$$c_{LR} = \frac{\pi}{4} \cdot \prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \left(1 - \frac{1}{p^2}\right)^{1/2} \approx 0.76422...$$

is the Landau-Ramanujan constant. On average, one has

$$\sum_{m \leq X} \mathcal{N}_m = \pi X + E(X),$$

where the estimation of the error term is known as the Gauss circle problem. Hardy proved that $E(X) \neq o(X^{1/4} \log^{1/4} X)$ [39], and he conjectured that $E(X) = O(X^{1/4+\epsilon})$ $\forall \epsilon > 0$. The best known upper bound [1] is $E(X) = O(X^{\alpha+\epsilon})$, where $\alpha = \frac{131}{416} \approx 0.31$ [41]. For our purposes, it is more significant to average $\mathcal{N}$

[1]After the submission of this thesis Bourgain and Watt have improved the exponent to 517/1648 [13].

over $S^{(2)}$ instead of over $\mathbb{N}$ (2.2.5):

$$\frac{1}{|\{m \in S^{(2)} : m \le X\}|} \sum_{\substack{m \le X \\ m \in S^{(2)}}} \mathcal{N}_m \sim c' \sqrt{\log X}.$$

Moreover, one has [47, section 7]

$$|\{m \in S^{(2)} : m \le X,\ \log \mathcal{N}_m \gg \log\log m\}| = |\{m \in S^{(2)} : m \le X\}| \cdot (1 + o(1))$$

so that $\mathcal{N} \to \infty$ for a density 1 sequence of energy levels.

Angular distribution.

Definition 2.2.3. Given an integer m which is the sum of d squares, define

$$\widehat{\mathcal{E}}_m := \frac{1}{\sqrt{m}} \mathcal{E}_m \subset \mathcal{S}^{d-1} \tag{2.2.6}$$

to be the projection of the set of lattice points on the unit sphere (cf. [12, (1.5)] and [62, (4.3)]).

As mentioned in section 1.1, for $d = 2$ the projected lattice points $\widehat{\mathcal{E}}_m$ equidistribute [30, 31] on the unit circle for generic sequences of energy levels. Equivalently, for a density one sequence of energies, the real numbers θ_μ, where

$$\mu = \|\mu\| \cdot e^{i\theta_\mu} = \sqrt{m} \cdot e^{i\theta_\mu}, \tag{2.2.7}$$

are equidistributed (mod 2π) in the sense of Definition 2.1.1. Indeed, the following proposition, due to Fainsilber, Kurlberg, and Wennberg, shows equidistribution *on average* of lattice points on circles (after applying Weyl's criterion, Proposition 2.1.2).

Proposition 2.2.4 ([31, Proposition 6]). *Let k be a non-zero integer with $4 \mid k$. Then there exist constants C, C' such that for X sufficiently big and $\log |k| \le C' \sqrt{\log X}$,*

$$\log \left(\frac{1}{X} \sum_{1 \le m \le X} \left| \sum_{\mu \in \mathcal{E}_m} e^{ik\theta_\mu} \right| \right) \le C - \left(1 - \frac{2}{\pi}\right) \log \left(\frac{\log X}{(\log |k|)^2} \right)$$

where θ_μ is defined by (2.2.7).

To the other extreme, Cilleruelo proved that there exist (thin) sequences of energy levels $\{m_k\}_k$ such that all the lattice points lie on arbitrarily short arcs:

$$\tau_{m_k} \Rightarrow \frac{1}{4}(\delta_{\pm 1} + \delta_{\pm i}), \tag{2.2.8}$$

with τ_m as in (1.2.9). The limiting measure in (2.2.8) is called the 'Cilleruelo measure' [20, 61, 47, 59]. Indeed, one has the following result.

Proposition 2.2.5 ([20, Theorem 2])**.** *For every $\epsilon > 0$ and for every integer k, there exists a circle $\sqrt{m}\mathcal{S}^1$ such that all the lattice points of $\mathcal{E}_m$ are on the arcs $\sqrt{m}e^{i\pi/2(t+\theta)}$, $|\theta| < \epsilon$, $t = 0, 1, 2, 3$, and $\mathcal{N}_m > k$.*

The weak-* partial limits of $\{\tau_m\}$ ("attainable measures") were partially classified in [47, 49].

The maximal number of lattice points on a short arc. As mentioned in section 1.2, Jarnik [45] showed that there exists $c > 0$ such that on any arc of length $< c(\sqrt{m})^{1/3}$ of the circle $\sqrt{m}\mathcal{S}^1$ there are at most 2 lattice points. Moreover, Cilleruelo-Córdoba [19] proved that, for all integers $l \geq 1$, on any arc of length $\leq \sqrt{2}(\sqrt{m})^{\frac{1}{2} - \frac{1}{(4\lfloor l/2 \rfloor + 2)}}$ there are at most l lattice points.

Proposition 2.2.6 (Bourgain and Rudnick [11, Lemma 2.1])**.** *On any arc of length at most $(\sqrt{m})^{\frac{1}{2}}$ of a circle of radius $\sqrt{m}$, there are $O(\log m)$ lattice points.*

Conjecture 2.2.7 (Cilleruelo and Granville [22, 21])**.** *Consider a circle of radius $\sqrt{m}$. For all $\delta > 0$, there exists a constant C_δ such that on any arc of length $(\sqrt{m})^{1-\delta}$ there are at most C_δ lattice points.*

Note that Conjecture 2.2.7 implies Conjecture 1.2.7. Bourgain and Rudnick [8, Lemma 5] (recall Lemma 1.2.4) showed that Conjecture 2.2.7 is true for a density one subsequence of $S^{(2)}$ (also bearing in mind (2.2.5)).

Lattice points on spheres $\sqrt{m}\mathcal{S}^2$

In this section, we assume $d = 3$. An integer m is representable as a sum of three squares if and only if it is not of the form $4^l(8k+7)$, for k, l non-negative integers [38, 24]. The set of energies

$$\mathcal{S}^{(3)} := \{0 < m : \ m = a_1^2 + a_2^2 + a_3^2, \ a_1, a_2, a_3 \in \mathbb{Z}\}$$

is of asymptotic density 5/6 in the integers [50, 68].

The total number of lattice points $\mathcal{N}^{(3)} = r_3(m)$ oscillates: it is unbounded but vanishes for arbitrarily large m. We have the upper bound [12, section 1]

$$\mathcal{N} \ll (\sqrt{m})^{1+\epsilon} \quad \text{for all } \epsilon > 0.$$

The condition $m \not\equiv 0, 4, 7 \pmod 8$ is equivalent to the existence of *primitive* lattice points $(\mu^{(1)}, \mu^{(2)}, \mu^{(3)})$, meaning $\mu^{(1)}, \mu^{(2)}, \mu^{(3)}$ are coprime (see e.g. [12, section 1] and [62, section 4]). In this case, we have both lower and upper bounds (recall (1.3.5))

$$(\sqrt{m})^{1-\epsilon} \ll \mathcal{N} \ll (\sqrt{m})^{1+\epsilon}$$

This lower bound is ineffective: the behaviour of $r_3(m)$ is not completely understood ([12, section 1]).

Equidistribution. Linnik conjectured (and proved under GRH) that the projected lattice points (2.2.6) on the unit sphere $\mathcal{S}^2$ become equidistributed as $m \to \infty$, $m \not\equiv 0, 4, 7 \pmod 8$. This result was proven unconditionally by Duke [27, 28], and by Golubeva and Fomenko [35], following a breakthrough by Iwaniec [43]. As a consequence, one may approximate a summation over the lattice point set by an integral over the unit sphere.

Lemma 2.2.8 (cf. [55, Lemma 8])**.** *Let $g(z)$ be a C^2-smooth function on $\mathcal{S}^2$. For $m \to \infty$, $m \not\equiv 0, 4, 7 \pmod 8$, we have*

$$\frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} g\left(\frac{\mu}{\|\mu\|}\right) = \int_{z \in \mathcal{S}^2} g(z) \frac{dz}{4\pi} + O_g\left(\frac{1}{m^{1/28-\epsilon}}\right).$$

Randomness on smaller scales. Bourgain, Sarnak and Rudnick [12] investigated the behaviour on smaller scales of the projected lattice points $\widehat{\mathcal{E}}_m \subset \mathcal{S}^2$ (2.2.6), giving evidence that they behave like random points. We now introduce one of the statistics they considered.

Definition 2.2.9. For $s > 0$, the **Riesz s-energy** of n (distinct) points $P_1, \dots, P_n$ on $\mathcal{S}^2$ is defined as

$$E_s(P_1, \dots, P_n) := \sum_{i \neq j} \frac{1}{\|P_i - P_j\|^s}.$$

Bourgain, Sarnak and Rudnick computed the following precise asymptotics for the Riesz s-energy of the projected lattice points.

Proposition 2.2.10 ([12, Theorem 1.1], [62, Theorem 4.1])**.** *Fix $0 < s < 2$. Suppose $m \to \infty$, $m \not\equiv 0, 4, 7 \pmod 8$. There is some $\delta > 0$ so that*

$$E_s(\widehat{\mathcal{E}}_m) = I(s) \cdot \mathcal{N}^2 + O(\mathcal{N}^{2-\delta})$$

where

$$I(s) = \frac{2^{1-s}}{2-s}.$$

Lattice points on spheres $\sqrt{m}\mathcal{S}^{d-1}$ with $d \geq 4$

For $d \geq 4$, every positive integer corresponds to an energy level (recall Theorem 2.2.1). In dimension 4 the number of lattice points still oscillates rather wildly [31, section 2]. Indeed, we have (see e.g. [37, (3.9)], or [64, (1.1.6)])

$$r_4(m) = 8 \sum_{d \mid m,\ 4 \nmid d} d,$$

hence, in particular, $r_4(2^l) = 24$ for every $l \geq 2$. For $d \geq 5$, we have the sharp bounds

$$m^{d/2-1} \ll \mathcal{N}^{(d)} \ll m^{d/2-1}, \tag{2.2.9}$$

as $m \to \infty$.

The projected lattice points on $\mathcal{S}^{d-1}$, $d \geq 4$, are equidistributed as $m \to \infty$. This is similar to the case $d = 3$, and in contrast with what happens when $d = 2$ (see section 2.2.2).

Lemma 2.2.11 ([44, Proposition 11.4], [58])**.** *Let $d \geq 4$, and $g(z)$ be a C^2-smooth function on $\mathcal{S}^{d-1}$. As $m \to \infty$, we have*

$$\sum_{\mu \in \mathcal{E}} g\left(\frac{\mu}{\|\mu\|}\right) = \mathcal{N} \cdot \int_{z \in \mathcal{S}^{d-1}} g(z) \frac{dz}{vol(\mathcal{S}^{d-1})} + O_g\left(m^{\frac{d-1}{4}+\epsilon}\right). \tag{2.2.10}$$

Corollary 2.2.12. *Let $d \geq 5$, and $g(z)$ be a C^2-smooth function on $\mathcal{S}^{d-1}$. As $m \to \infty$, we have*

$$\frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} g\left(\frac{\mu}{\|\mu\|}\right) = \int_{z \in \mathcal{S}^{d-1}} g(z) \frac{dz}{vol(\mathcal{S}^{d-1})} + O_g\left(m^{-\frac{d-3}{4}+\epsilon}\right).$$

Proof. Substitute (2.2.9) into (2.2.10). □

For each positive integer k, define the k-th moment of the normalised inner product of two lattice points

$$B_m^{(d)}(k) := \frac{1}{m^k \mathcal{N}^2} \sum_{\mu_1, \mu_2 \in \mathcal{E}^{(d)}} \langle \mu_1, \mu_2 \rangle^k. \tag{2.2.11}$$

Until the end of this section, assume $d \geq 3$. Each $B(k)$ has a unique limit as $m \to \infty$, due to the equidistribution of lattice points on spheres. Fix the notation

$$E(d) = \begin{cases} -1/28 + o(1) & d = 3 \\ -\frac{d-3}{4} + o(1) & d \geq 4. \end{cases}$$

The following result is a generalisation of Lemma 5.2.1 to higher dimensions (see Benatar, M. [4, Lemma 2.5]).

Lemma 2.2.13 (M.)**.** *For $d \geq 3$, we have*

$$B^{(d)}(k) = \begin{cases} 1 & \textit{for } k = 0; \\ 0 & \textit{for odd } k; \\ 1/d & \textit{for } k = 2; \\ \frac{\Gamma(d/2)\Gamma((k+1)/2)}{\Gamma((d+k)/2)\sqrt{\pi}} + O\left(m^{E(d)}\right) & \textit{for even } k \geq 4. \end{cases}$$

Proof. The case $k = 0$ is clear. For odd k, the summands of (2.2.11) cancel out in pairs, by the symmetry of the set $\mathcal{E}$ (Lemma 2.2.2). The case $k = 2$ follows directly from (2.2.2). It remains to prove the case of even $k \geq 4$. We begin by rewriting

$$B(k) = \frac{1}{\mathcal{N}^2} \sum_{\mu_1,\mu_2} (\cos(\varphi_{\mu_1,\mu_2}))^k,$$

where φ_{μ_1,μ_2} is the angle between μ_1 and μ_2. It suffices to prove that, for all μ_1, we have

$$\frac{1}{\mathcal{N}} \sum_{\mu_2} (\cos(\varphi_{\mu_1,\mu_2}))^k = \frac{\Gamma(d/2)\Gamma((k+1)/2)}{\Gamma((d+k)/2)\sqrt{\pi}} + O\left(m^{E(d)}\right). \tag{2.2.12}$$

To show (2.2.12), apply Lemma 2.2.8 with $g(\cdot) = \cos^k(\varphi_{\mu_1,\cdot})$:

$$\frac{1}{\mathcal{N}} \sum_{\mu_2} (\cos(\varphi_{\mu_1,\mu_2}))^k = \int_{z\in\mathcal{S}^{d-1}} (\cos(\varphi_{\mu_1,z}))^k \frac{dz}{\mathrm{vol}(\mathcal{S}^{d-1})} + O\left(m^{E(d)}\right). \tag{2.2.13}$$

We introduce the $d-1$ spherical coordinates $0 \leq \phi_1, \phi_2, \ldots, \phi_{d-2} \leq \pi$ and $0 \leq \phi_{d-1} \leq 2\pi$, and write

$$\begin{aligned} z = (&\cos(\phi_1), \sin(\phi_1)\cos(\phi_2), \sin(\phi_1)\sin(\phi_2)\cos(\phi_3), \ldots, \\ &\sin(\phi_1)\sin(\phi_2)\ldots\sin(\phi_{d-1})). \end{aligned}$$

The volume element is

$$dz = \sin^{d-2}(\phi_1)\sin^{d-3}(\phi_2)\ldots\sin(\phi_{d-2})d\phi_1\ldots d\phi_{d-1}.$$

We have $\mathrm{vol}(\mathcal{S}^{d-1}) = 2\pi^{d/2}/\Gamma(d/2)$. As the uniform probability measure on $\mathcal{S}^{d-1}$ is rotation invariant, the integral in (2.2.13) is independent of μ_1, and therefore equals

$$\int_{z\in\mathcal{S}^{d-1}} (\cos(\varphi_{(0,\dots,0,1),z}))^k \frac{dz}{\mathrm{vol}(\mathcal{S}^{d-1})}$$
$$= \frac{\Gamma(d/2)}{2\pi^{d/2}} \int_0^{2\pi} \sin^k(\phi_{d-1}) d\phi_{d-1} \cdot \prod_{j=1}^{d-2} \int_0^{\pi} \sin^{k+d-1-j}(\phi_j) d\phi_j. \quad (2.2.14)$$

For j an even positive integer, one has

$$\int_0^{2\pi} \sin^j(\phi) d\phi = 2\int_0^{\pi} \sin^j(\phi) d\phi = \frac{\sqrt{\pi}\cdot\Gamma((j+1)/2)}{\Gamma((j+2)/2)},$$

so that the RHS of (2.2.14) equals

$$\frac{\Gamma(d/2)}{2\pi^{d/2}} \cdot 2\sqrt{\pi}^{d-1} \prod_{j=1}^{d-1} \frac{\Gamma((k+d-j)/2)}{\Gamma((k+d+1-j)/2)} = \frac{\Gamma(d/2)\Gamma((k+1)/2)}{\Gamma((d+k)/2)\sqrt{\pi}}.$$

Replacing the latter equality into (2.2.14) and then into (2.2.13) yields (2.2.12). □

In particular, we record that

$$B^{(3)}(k) = \frac{1}{k+1} + O\left(m^{-1/28+o(1)}\right) \qquad \text{for even } k \geq 4, \quad (2.2.15)$$

and that

$$B^{(d)}(4) = \frac{3}{d(d+2)} + O(m^{E(d)}) \qquad \text{for } d \geq 3.$$

Correlations of lattice points on spheres

We consider the arithmetic problem of ℓ-tuples of lattice points on spheres $\sqrt{m}\mathcal{S}^{d-1}$ summing up to 0, focusing on the case of even ℓ (also see section 1.4).

Definition 2.2.14. For $\ell \geq 2$, the *set of d-dimensional ℓ-th lattice point correlations*, or ℓ-**correlations** for short, is

$$\mathcal{C}_m^{(d)}(\ell) := \left\{ (\mu_1, \dots, \mu_\ell) \in \mathcal{E}_m^{(d)^\ell} : \sum_{i=1}^{\ell} \mu_i = 0 \right\}.$$

The set of **non-degenerate** ℓ-correlations is

$$\mathcal{X}_m^{(d)}(\ell) := \left\{ (\mu_1, \dots, \mu_\ell) \in \mathcal{C}_m^{(d)}(\ell) : \forall \mathcal{H} \subsetneq \{1, \dots, \ell\}, \sum_{i \in \mathcal{H}} \mu_i \neq 0 \right\}.$$

Denote by $\mathcal{D} = \mathcal{D}_m^{(d)}(\ell)$ the set of **degenerate** correlations so that

$$\mathcal{C} = \mathcal{D} \dot{\cup} \mathcal{X}.$$

For even ℓ, we define the set of correlations $\mathcal{D}'$ that cancel out in pairs, of the form

$$\{\mu_1, -\mu_1, \dots, \mu_{\ell/2}, -\mu_{\ell/2}\}$$

and their permutations, and call these **symmetric** correlations [2]. Further, for even ℓ, denote by $\mathcal{D}''$ the set of **diagonal** correlations of the form

$$\{\pm\mu, \dots, \pm\mu\}$$

(with exactly $\ell/2$ plus signs).

We now review a few prior results on spectral correlations (also see [47, section 2.3]). Firstly, note that for every d and even ℓ we have

$$\mathcal{D}'' \subseteq \mathcal{D}' \subseteq \mathcal{D}.$$

A combinatorial argument shows that, for such d and even ℓ we have

$$|\mathcal{D}'^{(d)}_m(\ell)| \sim a_\ell \mathcal{N}_m^{\ell/2}, \tag{2.2.16}$$

[2] This terminology, employed to be consistent with [4], might be non-standard.

where $a_\ell := \mathbb{E}[Z^\ell] = (\ell-1)!!$ is the ℓ-th moment of a standard Gaussian random variable Z, and the double factorial is defined by

$$n!! := \prod_{k=0}^{\lceil n/2\rceil -1} (n-2k), \qquad n \in \mathbb{N}.$$

In particular from (2.2.16) we deduce for even ℓ the lower bound

$$|\mathcal{C}_m^{(d)}(\ell)| \gg \mathcal{N}_m^{\ell/2}.$$

For $\ell = 2$, it is easy to check that for every d

$$|\mathcal{C}_m^{(d)}(2)| = |\mathcal{D}''^{(d)}_m(2)| = \mathcal{N}_m^{(d)}. \tag{2.2.17}$$

In the rest of this section, let $d = 2$. For $\ell = 4$, as two circles intersect in at most two points ("Zygmund's trick" [74]), one has

$$|\mathcal{X}_m^{(2)}(4)| = 0 \qquad \text{for all } m \in S^{(2)}. \tag{2.2.18}$$

It follows that $\mathcal{C}^{(2)}(4) = \mathcal{D}'^{(2)}(4)$ (also using the trivial observation that $\mathcal{D}(4) = \mathcal{D}'(4)$ for every d).

For $\ell = 6$, by "Zygmund's trick", we have

$$|\mathcal{C}_m^{(2)}(6)| = O(\mathcal{N}^4)$$

as $\mathcal{N} \to \infty$. Bombieri and Bourgain established the stronger upper bound

$$|\mathcal{C}_m^{(2)}(6)| = O(\mathcal{N}^{7/2})$$

as $\mathcal{N} \to \infty$ via the Szemerédi-Trotter Theorem (see [6, section 2]).

The following result is also due to Bombieri-Bourgain. For $\ell \geq 6$ even and a density 1 sequence of energy levels $\{m\} \subset S^{(2)}$ it follows from [6, Theorem 17] (see also [7, Lemma 4]) that

$$|\mathcal{C}_m^{(2)}(\ell)| = a_\ell \mathcal{N}^{\ell/2} + O(\mathcal{N}^{\ell/2-1}) \qquad \text{as } \mathcal{N} \to \infty,$$

and also

$$|\mathcal{D}_m^{(2)}(\ell) \setminus \mathcal{D'}_m^{(2)}(\ell)| = O(\mathcal{N}^{\ell/2-1}), \qquad |\mathcal{X}_m^{(2)}(\ell)| = O(\mathcal{N}^{\ell/2-2}).$$

Hence, for $d = 2$, the symmetric tuples $\mathcal{D}'(\ell)$ are most of the set $\mathcal{C}(\ell)$, for 'generic' m.

2.3 Laplace eigenfunctions on the torus

Background

In this section, we prove Lemma 1.1.1. Consider the Helmholtz differential equation

$$(\Delta + E)G = 0,$$

with eigenvalue $E > 0$. On the torus $\mathbb{T}^d$, the Laplacian is given by

$$\Delta = \frac{\partial^2}{\partial x_1^2} + \frac{\partial^2}{\partial x_2^2} + \cdots + \frac{\partial^2}{\partial x_d^2}.$$

It is easy to check that, for each $\mu \in \mathbb{Z}^d$, the exponential $e^{2\pi i \langle \mu, x \rangle}$ is a Laplace eigenfunction, with eigenvalue

$$E = 4\pi^2 \sum_{i=1}^{d} (\mu^{(i)})^2.$$

Moreover, recall the general fact that the sum of two eigenfunctions in an eigenfunction if and only if they have the same eigenvalue (and in this case the sum has still the same eigenvalue). We now give some background on Hilbert spaces, needed to state the next lemmas. For more details, see e.g. Katznelson [46].

Complete orthonormal systems. In a Hilbert space, two vectors u, v are called *orthogonal* if $\langle u, v \rangle = 0$. A set of vectors is *orthogonal* if its elements are pairwise orthogonal. A complete orthonormal system is an orthogonal set $\{u_i\}_i$ consisting of norm one vectors, and such that the only vector orthogonal to every u_i is the zero vector.

Square integrable functions on the torus. The space $L^2(\mathbb{T}^d)$ of square integrable complex-valued functions on the torus is a Hilbert space, with scalar product given by

$$\langle F, G\rangle := \int_{\mathbb{T}^d} F(x)\overline{G(x)}dx.$$

The norm of a function is thus

$$\|F\|_2 = \sqrt{\langle F, F\rangle} = \sqrt{\int_{\mathbb{T}^d} \|F(x)\|_{\mathbb{C}}^2 dx}.$$

Proof of Lemma 1.1.1

Lemma 2.3.1 ([46, section I.5])**.** *The exponentials $\{e^{2\pi i\langle\mu,\cdot\rangle}\}_{\mu\in\mathbb{Z}^d}$ form a complete orthonormal system for the Hilbert space $L^2(\mathbb{T}^d)$ of square integrable functions on the torus.*

In $L^2(\mathbb{T}^d)$, let A be a function and $\{A_\mu\}_{\mu\in\mathbb{Z}^d}$ a collection of functions. We say that the series $\sum_\mu A_\mu$ *converges to A in the L^2 norm*, and write

$$A = \sum_\mu A_\mu,$$

if the sequence of partial sums

$$S_M(x) := \sum_{\substack{\mu\in\mathbb{Z}^d \\ \max_i\{|\mu_i|\}\le M}} A_\mu$$

satisfies

$$\|A - S_M\|_2 = \sqrt{\int_{\mathbb{T}^2} \|(A - S_M)(x)\|_{\mathbb{C}}^2 dx} \to 0$$

as $M \to \infty$.

Lemma 2.3.2 ([46, section I.5]). *In a Hilbert space, if $\{u_i\}_i$ is a complete orthonormal system, then every vector u may be uniquely written as*

$$u = \sum_i \langle u, u_i \rangle u_i,$$

where $\langle u, u_i \rangle$ are called Fourier coefficients.

Combining Lemmas 2.3.1 and 2.3.2, we obtain Lemma 1.1.1: each Laplace eigenfunction on $\mathbb{T}^d$ with eigenvalue $4\pi^2 m$ may be (uniquely) written as

$$G(x) = \sum_{\mu \in \mathcal{E}_m} g_\mu e^{2\pi i \langle \mu, x \rangle},$$

where $\mathcal{E}$ is given by (2.2.1), and the Fourier coefficients by

$$g_\mu = \langle G(x), e^{2\pi i \langle \mu, x \rangle} \rangle \in \mathbb{C}.$$

2.4 Random fields

Definitions

The results of the present section are borrowed from [2, 23, 1].

Gaussian processes. Recall that the probability density of the real Gaussian random variable $Y \sim N(m, \sigma^2)$ is

$$\phi_Y(y) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2}(\frac{y-m}{\sigma})^2}.$$

Definition 2.4.1. A random vector $(X_1, \dots, X_n)$ is *multivariate Gaussian* if, for every $v = (v_1, \dots, v_n) \in \mathbb{R}^n$, the real random variable $Y := \sum_{i=1}^n v_i X_i$ is Gaussian. For $(X_1, \dots, X_n)$ multivariate Gaussian, define the vector $m =$

$(m_1, \ldots, m_n)$ by $m_i = \mathbb{E}[X_i]$, and the positive semi-definite **covariance matrix** $C = \{c_{ij}\}$ by

$$c_{ij} = \mathbb{E}\left[(X_i - m_i)(X_j - m_j)\right].$$

If C is positive definite, the multivariate Gaussian distribution is called **non-degenerate**. The probability density function of $(X_1, \ldots, X_n)$ is given by

$$\phi_{X_1,\ldots,X_n}(x) = \frac{1}{\sqrt{(2\pi)^n \det C}} \exp\left(-\frac{1}{2}(x-m)^T C^{-1}(x-m)\right). \tag{2.4.1}$$

If the mean is zero, the distribution is called *centred*.

A Gaussian distribution is thus completely determined by its mean vector and covariance matrix. In the rest of this section, we will analyse properties of **processes** p with *parameter set* $T \subset \mathbb{R}$ ($t \in T$ may represent e.g. values of 'time') [3]. We always assume that the $p(t)$, called the *realisations* or *sample paths* of our process, are almost surely [4] continuous in t. The properties presented below generalise almost verbatim to the multidimensional case of **random fields**, where $T \subset \mathbb{R}^n$. For simplicity of exposition, we shall give the statements for processes. We will always assume all processes and fields to be real-valued.

Definition 2.4.2. A process $p = (p_t)_t$, $t \in T$, is *Gaussian* if, for all $k = 1, 2 \ldots$ and every $t_1, \ldots, t_k \in T$, the random vectors

$$(p(t_1), \ldots, p(t_k)),$$

called *finite-dimensional distributions* of p, are multivariate Gaussian.

Covariance function. For a process p, we define its *expectation function* $\mathbb{E}[p(t)] =: \nu(t)$. We may always assume our process p to be *centred* (i.e., $\nu \equiv 0$) by considering the process $p(t) - \nu(t)$.

[3] For an underlying probability space $(\Omega, \mathcal{F}, \mathbb{P})$, we define $p : \Omega \times T \to \mathbb{R}$.

[4] The expression 'almost surely', or for short 'a.s.', means 'with probability 1'.

Definition 2.4.3. Given a centred process p, we define its *covariance function*:

$$\mathbb{E}[p(t)p(u)] =: r(t,u).$$

Lemma 2.4.4 ([23, §5.1])**.** *Given a centred finite-variance process, its covariance function is always nonnegative definite, in the sense that for all positive k, every $t_1, \ldots, t_k \in T$ and any choice of real numbers $x_1, \ldots, x_k$, one has*

$$\sum_{i,j=1}^{k} r(t_i, t_j) x_i x_j \geq 0.$$

Proof. Indeed, one has

$$\sum_{i,j=1}^{k} r(t_i, t_j) x_i x_j = \mathbb{E}\left[\sum_{i,j=1}^{k} p(t_i) p(t_j) x_i x_j\right] = \mathbb{E}\left[\left(\sum_{i=1}^{k} p(t_i) x_i\right)^2\right] \geq 0$$

(see [23, (5.1.4)]). □

A centred Gaussian process may be completely described by its covariance function (see Kolmogorov's Theorem [23, section 3.3] or [2, section 1.2]).

Stationary processes.

Definition 2.4.5. A process p is *strictly stationary* if its finite-dimensional distributions are invariant for any time translation τ:

$$(p(t_1 + \tau), \ldots, p(t_k + \tau)) = (p(t_1), \ldots, p(t_k)).$$

Equivalently, for all $k = 1, 2, \ldots$, all $t_1, \ldots, t_k \in T$, any τ so that $\tau + t_i \in T$ for $1 \leq i \leq k$, and any $x_1, \ldots, x_k \in \mathbb{R}$, one has

$$\mathbb{P}\left(p(t_1 + \tau) \leq x_1, \ldots, p(t_k + \tau) \leq x_k\right) = \mathbb{P}\left(p(t_1) \leq x_1, \ldots, p(t_k) \leq x_k\right).$$

Definition 2.4.6. A (centred) process p is *stationary* if

$$\mathbb{E}[p(t)p(u)] = r(t-u),$$

i.e. the covariance function depends only on the time difference $t - u$.

If a (centred) process is real and Gaussian, then stationarity and strict stationarity are equivalent conditions [23, section 7.1].

The covariance function of arithmetic random waves

The arithmetic random wave (1.1.4)

$$F_m^{(d)}(x) = \frac{1}{\sqrt{\mathcal{N}_m^{(d)}}} \sum_{\mu \in \mathcal{E}^{(d)}} a_\mu e^{2\pi i \langle \mu, x \rangle}, \qquad x \in \mathbb{T}^d,$$

is a centred **stationary Gaussian random field**: indeed, its covariance function is given by

$$r_F^{(d)}(x,y) := \mathbb{E}[F(x) \cdot F(y)] = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i \langle \mu, (x-y) \rangle}, \tag{2.4.2}$$

depending on $x - y$ only. With abuse of notation, we might also write $r(x)$. We record that for any point x, one has $|r(x)| \leq 1$. Moreover, $r(0) = 1$, i.e., F is unit variance. We shall also need the following result.

Proposition 2.4.7 ([60, Proposition 2.4], [54, Lemma 2.2])**.** *Except for finitely many $x \in \mathbb{T}^d$, we have*

$$|r(x)| < 1.$$

Covariance function of the process $F(\gamma)$. We now consider the restriction of F to a smooth curve $\mathcal{C} \subset \mathbb{T}^d$, with arc-length parametrisation given by $\gamma(t) : [0, L] \to \mathbb{T}^d$. We obtain the process $f^{(d)} : [0, L] \to \mathbb{R}$,

$$f^{(d)}(t) := F(\gamma(t)) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{\mu \in \mathcal{E}} a_\mu e^{2\pi i \langle \mu, \gamma(t) \rangle}. \tag{2.4.3}$$

In what follows, we will be naturally led to studying the process f, as the nodal intersections (1.2.6) and (1.3.4) (for $d = 2, 3$ respectively) are counted by the zeros of $f^{(d)}$ (see sections 3.1 and 4.1). Note that f is (in general) non-stationary: we may see this by writing its covariance function

$$r^{(d)}(t_1, t_2) = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i \langle \mu, \gamma(t_1) - \gamma(t_2) \rangle}. \tag{2.4.4}$$

Now assume $\mathcal{C} \subset \mathbb{T}^d$ to be a straight line segment $\gamma(t) = t\alpha$, with $\alpha \in \mathbb{R}^d$ and $\|\alpha\| = 1$. We may thus rewrite (2.4.3) as

$$f(t) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{\mu \in \mathcal{E}} a_\mu e^{2\pi i t \langle \mu, \alpha \rangle}, \tag{2.4.5}$$

and its covariance function (2.4.4) as

$$r(t_1, t_2) = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i (t_1 - t_2) \langle \mu, \alpha \rangle}. \tag{2.4.6}$$

The process (2.4.5) is stationary: indeed, (2.4.6) depends on the difference $t_1 - t_2$ only.

Moments of the covariance function and spectral correlations. For $\ell \geq 0$, define the ℓ-th moment of the covariance function (2.4.2) as follows:

$$\mathcal{R}(\ell) = \mathcal{R}_m^{(d)}(\ell) := \int_{\mathbb{T}^d} |r_F^\ell(x)| dx. \tag{2.4.7}$$

For ℓ even, the moments (2.4.7) are related to the ℓ-correlations of Definition 2.2.14:

$$\mathcal{R}_m^{(d)}(\ell) = \frac{|\mathcal{C}_m^{(d)}(\ell)|}{\mathcal{N}^\ell},$$

as pointed out for instance in [47, section 2.3].

Kac-Rice formulas for the number of zeros

The problems presented in sections 1.2 and 1.3 require counting the number of zeros of the process (2.4.5) (respectively for $d = 2, 3$), as detailed in section 3.2. For a process p satisfying appropriate assumptions, moments of the number of zeros, and more generally moments of the number of *crossings of a level* u

$$\sigma_u(p, T) := |\{t \in T : p(t) = u\}|,$$

may be computed via **Kac-Rice formulas** [2, 23, 1]. The nodal area (see section 1.4) is a higher dimensional analogue of the zero crossings: to study the moments of the nodal area, we will need Kac-Rice formulas for random fields, computing the moments of the *geometric measure* of a level set [2, 1] (see section 2.4.4).

Let $p : I \to \mathbb{R}$ be a (a.s. C^1-smooth, say) Gaussian process on an interval $I \subseteq \mathbb{R}$. For $j \geq 1$ and distinct points $t_1, \ldots, t_j \in I$, consider the probability density function (recall Definition 2.4.1)

$$\phi_{p(t_1),\ldots,p(t_j)}$$

of the Gaussian random vector

$$(p(t_1), \ldots p(t_j)) \in \mathbb{R}^j.$$

For distinct points $t_1, \ldots, t_j$, define the **j-th zero-intensity** of p to be the conditional Gaussian expectation

$$\begin{aligned} &K_j(t_1, \ldots, t_j) \\ &\qquad = \phi_{p(t_1),\ldots,p(t_j)}(0, \ldots, 0) \cdot \mathbb{E}\left[|p'(t_1) \ldots p'(t_j)| \;\middle|\; p(t_1) = 0, \ldots, p(t_j) = 0\right], \end{aligned}$$

where p' denotes the first derivative of p. In the Gaussian setting, we have

$$\phi_{p(t_1),\ldots,p(t_j)}(0, \ldots, 0) = \frac{1}{\sqrt{(2\pi)^j \det(A)}}$$

(2.4.1), where A is the covariance matrix of $(p(t_1), \ldots, p(t_j))$. We will make use especially of the first and second intensities, also called respectively **zero density** function $K_1 : I \to \mathbb{R}$,

$$K_1(t) = \phi_{p(t)}(0) \cdot \mathbb{E}[|p'(t)| \bigm| p(t) = 0], \tag{2.4.8}$$

and **2-point correlation** function $\tilde{K_2} : I \times I \to \mathbb{R}$,

$$\tilde{K_2}(t_1, t_2) = \phi_{p(t_1),p(t_2)}(0, 0) \cdot \mathbb{E}[|p'(t_1)| \cdot |p'(t_2)| \bigm| p(t_1) = p(t_2) = 0], \tag{2.4.9}$$

the latter defined for $t_1 \neq t_2$. The notation is $\tilde{K_2}$ rather than K_2, as we will be working mostly with a scaled version of the two-point function, which shall be denoted K_2.

Theorem 2.4.8 (Kac-Rice formulas for the number of zeros [2, Theorem 3.2], [62, Theorem 2.1], [23, section 10])**.** *Let p be a real-valued Gaussian process defined on an interval $I \subseteq \mathbb{R}$ and having C^1 paths. Denote $\mathcal{Z}$ the number of zeros of p on I. Let j be a positive integer. Assume that for every j* pairwise distinct *points $t_1, \dots t_j \in I$ the joint distribution of $(p(t_1), \dots, p(t_j)) \in \mathbb{R}^j$ is non-degenerate. Then*

$$\mathbb{E}[\mathcal{Z}^{[j]}] = \int_{I^j} K_j(t_1, \dots t_j) dt_1 \dots dt_j, \tag{2.4.10}$$

where

$$\mathcal{Z}^{[j]} = \begin{cases} \mathcal{Z}(\mathcal{Z}-1)\cdots(\mathcal{Z}-j+1) & \text{if } \mathcal{Z} \geq j \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

We note that, under the assumption that p is a stationary process, the above formulas simplify: in particular, the zero density (2.4.8) is a constant function $K_1(t) \equiv K_1$, and (2.4.9) becomes

$$\tilde{K_2}(t) = \phi_{p(0),p(t)}(0,0) \cdot \mathbb{E}[|p'(0)| \cdot |p'(t)| \mid p(0) = p(t) = 0]. \tag{2.4.11}$$

As remarked in [62], the Kac-Rice formulas as presented in the classical treatise [23] require the joint distribution of the $2j$-dimensional random vector

$$(p(t_1), \dots, p(t_j), p'(t_1), \dots, p'(t_j))$$

to be non-degenerate. This condition was weakened in [2] to require only the non-degeneracy of

$$(p(t_1), \dots, p(t_j)),$$

as in the hypotheses of Theorem 2.4.8.

Kac-Rice formulas for the geometric measure of the zero set

Given a smooth random field P with parameter set $T \subset_{\text{open}} \mathbb{R}^d$ and having values in $\mathbb{R}^{d'}$, let $\mathcal{V}$ be the *geometric measure* [5] of its zero set. When $d - d' = 0$, $\mathcal{V}$ is the number of zeros, as in the previous case. When $d - d' = 1$, $\mathcal{V}$ is the nodal length of P; when $d - d' = 2$, $\mathcal{V}$ is the nodal area, and so forth (recall the terminology in section 1.1). In chapter 5 we will be concerned with the case $d = 3$, $d' = 1$. Only the case $d \geq d'$ is interesting, since otherwise the zero set of P is a.s. empty. One may compute, under appropriate assumptions, the moments of $\mathcal{V}$ by means of Kac-Rice formulas [2, Theorems 6.2, 6.3, 6.8 and 6.9].

For every $u \in \mathbb{R}^{d'}$, the *u-level set* of the random field P is

$$C_u(P, T) := \{t \in T : P(t) = u\}.$$

The nodal set is of course the 0-level set. The level set is a.s. a C^1-smooth manifold of dimension $d - d'$ [2, section 6.2]. Denote $\sigma_u(P, T)$ the geometric measure of $C_u(P, T)$. In the following statement, P' indicates the Jacobian matrix of P, and $*$ is the transpose operator.

Proposition 2.4.9 (Kac-Rice formula for the expectation of the geometric measure of a level set [2, Theorems 6.8])**.** *Let P be a random field with parameter set $T \subset_{open} \mathbb{R}^d$ and values in $\mathbb{R}^{d'}$, and $u \in \mathbb{R}^{d'}$ a fixed point. Assume that:*

(i) P is Gaussian.

(ii) Almost surely the function $t \rightsquigarrow P(t)$ is of class C^1.

(iii) For each $t \in T$, $P(t)$ has a non-degenerate distribution.

(iv) It also holds that

$$\mathbb{P}(\exists t \in T : P(t) = u \text{ and } P'(t) \text{ does not have full rank}) = 0.$$

[5] For the definition of geometric measure see e.g. [32, §2.10.15].

Then, for every Borel set B contained in T, one has

$$\mathbb{E}[\sigma_u(P,B)] = \int_B \mathbb{E}\left[\det(P'(t)P'(t)^*)^{1/2} \;\middle|\; P(t)=u\right] \cdot \phi_{P(t)}(u)dt. \tag{2.4.12}$$

If B is compact, both sides in (2.4.12) *are finite.*

The integrand in (2.4.12) with $d'=1$ and $u=0$ simplifies to $K_1 : T \to \mathbb{R}$,

$$K_1(t) := \mathbb{E}\left[\|\nabla P(t)\| \;\middle|\; P(t)=0\right] \cdot \phi_{P(t)}(0). \tag{2.4.13}$$

The expression (2.4.13) is called the zero density of the random field P, the higher dimensional analogue of (2.4.8).

Proposition 2.4.10 (Kac-Rice formula for the j-th moment of the geometric measure of a level set [2, Theorem 6.9])**.** *Let $j \geq 2$ be an integer. Assume the same hypotheses as in Proposition 2.4.9 except for (iii) that is replaced by*

(iii)′ For distinct values $t_1,\ldots,t_j \in T$, the distribution of

$$(P(t_1),\ldots,P(t_j))$$

does not degenerate in $(\mathbb{R}^{d'})^j$.

Then, for every Borel set B contained in T and levels $u_1,\ldots,u_j$, one has

$$\mathbb{E}\left[\prod_{i=1}^{j}\sigma_{u_i}(P,B)\right] = \int_{B^j}\mathbb{E}\left[\prod_{i=1}^{j}\det(P'(t_i)P'(t_i)^*)^{1/2} \;\middle|\; P(t_1)=u_1,\ldots,\right.$$
$$\left. P(t_j)=u_j\right] \cdot \phi_{P(t_1),\ldots,P(t_j)}(u_1,\ldots,u_j)dt_1\ldots dt_j, \tag{2.4.14}$$

where both members may be infinite.

The integrand in (2.4.14) with $d'=1$, $j=2$ and $u_1=u_2=0$ simplifies to $\tilde{K}_2 : T \times T \to \mathbb{R}$,

$$\tilde{K}_2(t_1,t_2) := \mathbb{E}\left[\|\nabla P(t_1)\| \cdot \|\nabla P(t_2)\| \;\middle|\; P(t_1)=P(t_2)=0\right] \cdot \phi_{P(t_1),P(t_2)}(0,0). \tag{2.4.15}$$

The expression (2.4.15) is called the two-point correlation function of P, the higher dimensional analogue of (2.4.9). In the stationary case, (2.4.15) simplifies further to read

$$\tilde{K}_2(t) = \mathbb{E}\left[\|\nabla P(0)\| \cdot \|\nabla P(t)\| \;\middle|\; P(0) = P(t) = 0\right] \cdot \phi_{P(0),P(t)}(0,0). \tag{2.4.16}$$

Chapter 3

Nodal intersections in 2D

The present chapter incorporates the publication [53]. We will prove Theorems 1.2.5, 1.2.6, 1.2.8 and 1.2.9.

3.1 Outline

We will work with the ensemble of arithmetic random waves on the two-dimensional torus (1.2.5),

$$F_m^{(2)}(x) = \frac{1}{\sqrt{\mathcal{N}_m^{(2)}}} \sum_{(\mu^{(1)},\mu^{(2)})\in\mathcal{E}} a_\mu e^{2\pi i\langle\mu,x\rangle}, \tag{3.1.1}$$

where we recall that

$$\mathcal{E} = \{\mu \in \mathbb{Z}^2 : \|\mu\|^2 = m\}$$

is the set of lattice points lying on the circle of radius $\sqrt{m}$, and $\mathcal{N} = |\mathcal{E}|$ is their number. We investigate the distribution of the nodal intersections number (1.2.6),

$$\mathcal{Z} = \mathcal{Z}_m^{(2)}(F) := |\{x \in \mathbb{T}^2 : F(x) = 0\} \cap \mathcal{C}|,$$

against a fixed straight line segment $\mathcal{C}$ (1.2.17),

$$\mathcal{C} : \gamma(t) = t(\alpha_1, \alpha_2), \quad 0 \leq t \leq L, \quad \alpha \in \mathbb{R}^2, \quad \|\alpha\| = 1,$$

as $m \to \infty$.

In section 3.2, thanks to the work of Rudnick and Wigman [61] for generic curves $\mathcal{C}$, we reduce the problem of studying the variance of $\mathcal{Z}$ to bounding the second moment of the covariance function of F restricted to $\mathcal{C}$ (2.4.4)

$$r(t_1, t_2) = \mathbb{E}[F(\gamma(t_1))F(\gamma(t_2))]$$

and a couple of its derivatives. Next, using the hypothesis that $\mathcal{C}$ is a segment, we further reduce our problem to bounding sums over lattice points on circles. This relies on estimates for the second moment (established in appendix A).

There are marked differences compared to the case of generic curves: firstly, if $\mathcal{C}$ is a line segment, the covariance function has the special form (2.4.6)

$$r(t_1, t_2) = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i (t_1 - t_2)\langle \mu, \alpha \rangle} \tag{3.1.2}$$

so that the process $f(t) = F(\gamma(t))$ is stationary (recall section 2.4.2). This leads to a different method from [61] of controlling the second moment, and specifically the off-diagonal terms of (A.1.4). Indeed, in [61, Lemma 5.2], the off-diagonal terms are handled via Van der Corput's lemma, applicable for curves $\mathcal{C}$ of nowhere vanishing curvature, whereas the special form (3.1.2) of the covariance function allows us to establish the estimate (A.1.7) directly; the latter term happens to be of different nature than the corresponding expression in the non-vanishing curvature case (cf. [61, (5.18)]). This leads to bounding a certain summation over the lattice points, different from [61]: Rudnick and Wigman proved that (see [61, Proposition 5.3])

$$\sum_{\substack{\mu, \mu' \in \mathcal{E} \\ \mu \neq \mu'}} \frac{1}{\|\mu - \mu'\|} \ll \mathcal{N}^{\epsilon}, \quad \forall \epsilon > 0,$$

whereas in this work, we need to bound

$$\sum_{\substack{\mu,\mu'\in\mathcal{E} \\ \langle\mu-\mu',\alpha\rangle\neq 0}} \frac{1}{\langle\mu-\mu',\alpha\rangle^2} \tag{3.1.3}$$

where α is the direction of our straight line. In section 3.3, we bound (3.1.3) for α rational, and complete the proof of Theorem 1.2.5; in section 3.4, we treat the irrational case, and complete the proofs of Theorems 1.2.6, 1.2.8 and 1.2.9.

3.2 An approximate Kac-Rice formula

Recall that the arithmetic random wave (3.1.1) is a centred stationary Gaussian random field (see section 2.4.2). For now we assume $\mathcal{C}$ to be a smooth toral curve (which may or may not be a segment). Let $\gamma(t) : [0, L] \to \mathbb{T}^2$ be its arc-length parametrisation. We restrict F along $\mathcal{C}$, which yields the (centred Gaussian) process f (2.4.3)

$$f(t) := F(\gamma(t)) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{\mu\in\mathcal{E}} a_\mu e^{2\pi i\langle\mu,\gamma(t)\rangle}. \tag{3.2.1}$$

As mentioned in section 2.4.2, the nodal intersections $\mathcal{Z}$ (1.2.6) are counted by the zeros of f. Then Theorem 2.4.8 with $j = 1$ gives us the Kac-Rice formula for the expectation

$$\mathbb{E}(\mathcal{Z}) = \int_0^L K_1(t)dt, \tag{3.2.2}$$

where we recall K_1 is the zero density (2.4.8) of f,

$$K_1(t) = \phi_{f(t)}(0) \cdot \mathbb{E}[\|f'(t)\| \big| f(t) = 0],$$

with $\phi_{f(t)}$ the Gaussian density of $f(t)$. Rudnick and Wigman proved that $K_1(t) \equiv \sqrt{2}\sqrt{m}$ (see [61, Lemma 2.1]), and via (3.2.2) they computed the expected intersection number to be $\sqrt{2m}L$ (1.2.11). This holds for all smooth toral curves, hence in particular for our setting of straight line segments.

We now turn to the nodal intersections variance. With the notation (2.4.9), the two-point correlation function of f is

$$\tilde{K}_2(t_1, t_2) = \phi_{f(t_1),f(t_2)}(0,0) \cdot \mathbb{E}[\|f'(t_1)\| \cdot \|f'(t_2)\| \mid f(t_1) = f(t_2) = 0],$$

with $\phi_{f(t_1),f(t_2)}$ the joint Gaussian density of the vector $(f(t_1), f(t_2))$. According to Theorem 2.4.8 with $j = 2$, if the distribution of $(f(t_1), f(t_2))$ is nondegenerate for all $(t_1, t_2) \in [0, L] \times [0, L]$ such that $t_1 \neq t_2$, then one has

$$\mathbb{E}(\mathcal{Z}^2 - \mathcal{Z}) = \int_0^L \int_0^L \tilde{K}_2(t_1, t_2) dt_1 dt_2. \tag{3.2.3}$$

This non-degeneracy condition may fail for f as in (3.2.1), and the Kac-Rice formula (3.2.3) for f is in general wrong, as illustrated in [61, section 1.3]; however, Rudnick and Wigman developed an **approximate Kac-Rice formula**. Denote

$$r_1 = \frac{\partial r(t_1, t_2)}{\partial t_1}, \qquad r_2 = \frac{\partial r(t_1, t_2)}{\partial t_2} \qquad \text{and} \quad r_{12} = \frac{\partial^2 r(t_1, t_2)}{\partial t_1 \partial t_2}$$

the derivatives of the covariance function (2.4.4).

Proposition 3.2.1 (Approximate Kac-Rice bound [62, Proposition 2.2]). *We have*

$$Var(\mathcal{Z}) = m \cdot O(\mathfrak{R}_2(m))$$

where

$$\mathfrak{R}_2(m) := \int_0^L \int_0^L \left(r^2 + \left(\frac{r_1}{\sqrt{m}} \right)^2 + \left(\frac{r_2}{\sqrt{m}} \right)^2 + \left(\frac{r_{12}}{m} \right)^2 \right) dt_1 dt_2. \tag{3.2.4}$$

This result is applicable to the case where $\mathcal{C}$ is a segment, as it holds for all smooth curves. Note that the approximate Kac-Rice formula [61, Proposition 1.3] gives both the leading term and the error term for the variance; the upper bound of Proposition 3.2.1 is sufficient for our purposes. Our initial problem is thus reduced to bounding the second moment of the covariance function and a couple of its derivatives along $\mathcal{C}$.

3.3 Rational lines: proof of Theorem 1.2.5

The goal of this section is to prove Theorem 1.2.5. Recall the notation of the lattice point set $\mathcal{E}$ and number $\mathcal{N}$. From this point on, assume $\mathcal{C} \subset \mathbb{T}^2$ to be a segment as in (1.2.17): then, the process f is stationary, with covariance function (3.1.2) (and without loss of generality we may assume that $\mathcal{C}$ contains the origin). We now further reduce our problem to bounding a sum over the lattice points.

Definition 3.3.1. Given a nonzero vector $v \in \mathbb{R}^2$, we define the set

$$A_v := \{(\mu, \mu') \in \mathcal{E}^2 : \langle \mu - \mu', v \rangle \neq 0\}.$$

Proposition 3.3.2. *Assuming $\mathcal{C}$ to be a segment, one has*

$$Var(\mathcal{Z}) \ll \frac{m}{\mathcal{N}} + \frac{m}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right).$$

The proof of Proposition 3.3.2 is given in appendix A. Assuming it, we need only to bound the summation

$$\sum_{A_\alpha} \frac{1}{\langle \mu - \mu', \alpha \rangle^2}.$$

We do this first for α rational.

Proposition 3.3.3. *Let $\alpha = (\alpha_1, \alpha_2)$ with $\alpha_2/\alpha_1 \in \mathbb{Q}$, and A_α be as in Definition 3.3.1. Then*

$$\sum_{A_\alpha} \frac{1}{\langle \mu - \mu', \alpha \rangle^2} \ll_\alpha \mathcal{N}. \tag{3.3.1}$$

Proof. Up to multiplication by a scalar, α has integer coordinates:

$$\alpha = (\alpha_1, \alpha_2) = \alpha_1 \left(1, \frac{\alpha_2}{\alpha_1}\right) = \alpha_1 \left(1, \frac{p}{q}\right) = \frac{\alpha_1}{q} \cdot (q, p)$$

for some $p, q \in \mathbb{Z}$ and $q \neq 0$. Note that $A_\alpha = A_{(q,p)}$ because the vectors α and (q, p) are collinear. It follows that

$$\sum_{A_\alpha} \frac{1}{\langle \mu - \mu', \alpha \rangle^2} = \frac{q^2}{\alpha_1^2} \cdot \sum_{A_{(q,p)}} \frac{1}{\langle \mu - \mu', (q,p) \rangle^2} \ll_\alpha \sum_{A_{(q,p)}} \frac{1}{\langle \mu - \mu', (q,p) \rangle^2}. \tag{3.3.2}$$

Next, let μ be fixed, and consider $k = \langle \mu - \mu', (q, p) \rangle$. As both $\mu - \mu'$ and (q, p) have integer coordinates, it follows that $k \in \mathbb{Z}$. Moreover, since $(\mu, \mu') \in A_{(q,p)}$, we have $k \neq 0$. Then

$$\sum_{A_{(q,p)}} \frac{1}{\langle \mu - \mu', (q,p) \rangle^2} = \sum_{\mu} \sum_{k \neq 0} \sum_{\substack{\mu' \\ \langle \mu - \mu', (q,p) \rangle = k}} \frac{1}{k^2}. \tag{3.3.3}$$

We now show that there are at most two terms in the inner-most summation: the lattice point μ' of the circle $x^2 + y^2 = m$ has to satisfy, for fixed μ and k,

$$\langle \mu', (q,p) \rangle = \langle \mu, (q,p) \rangle - k = \mu_1 q + \mu_2 p - k =: h.$$

Thus μ' is lying on the straight line $qx + py = h$, and a circle and a line can intersect in at most two points. Therefore,

$$\sum_{\mu} \sum_{k \neq 0} \sum_{\substack{\mu' \\ \langle \mu - \mu', (q,p) \rangle = k}} \frac{1}{k^2} \leq 2 \sum_{\mu} \sum_{k \neq 0} \frac{1}{k^2} = 2 \cdot \frac{\pi^2}{3} \mathcal{N} \ll \mathcal{N}. \tag{3.3.4}$$

Combining (3.3.2), (3.3.3) and (3.3.4) we get the statement (3.3.1) of Proposition 3.3.3. □

Proof of Theorem 1.2.5. Applying Proposition 3.3.2, we have

$$\mathrm{Var}(\mathcal{Z}) \ll \frac{m}{\mathcal{N}} + \frac{m}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \tag{3.3.5}$$

with A_α as in Definition 3.3.1. By Proposition 3.3.3,

$$\sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \ll \mathcal{N}$$

and the statement of Theorem 1.2.5 follows. □

3.4 The case of irrational lines

The goal of this section is to prove Theorems 1.2.6, 1.2.8 and 1.2.9.

Preparatory results

Recall that $\sqrt{m}\mathcal{S}^1$ is the radius $\sqrt{m}$ circle. To bound the summation (3.1.3)

$$\sum_{\substack{\mu,\mu'\in\mathcal{E} \\ \langle\mu-\mu',\alpha\rangle\neq 0}} \frac{1}{\langle\mu-\mu',\alpha\rangle^2} \tag{3.4.1}$$

we begin by proving (Lemma 3.4.1 below) that for fixed μ, if the quantity

$$\langle\mu-\mu',\alpha\rangle$$

is small, then μ' lies on a short arc of $\sqrt{m}\mathcal{S}^1$. We will then bound (3.4.1) in Proposition 3.4.2, assuming bounds for lattice points on short arcs,

Lemma 3.4.1. *Let $c = c(m) > 0$, with $c \to 0$ as $m \to \infty$. Fix a point $B \in \sqrt{m}\mathcal{S}^1$, and let β be a unit vector. Then there exists an arc $\overset{\frown}{DE}$ of $\sqrt{m}\mathcal{S}^1$ of length $(4c+O(c^3))\sqrt{m}$ such that all points $B' \in \sqrt{m}\mathcal{S}^1$ satisfying $B' \neq B$ and $|\langle B-B',\beta\rangle| \leq c\|B-B'\|$ lie on $\overset{\frown}{DE}$.*

Proof. The condition $|\langle B-B',\beta\rangle| \leq c\|B-B'\|$ means $B-B'$ and β are close to being orthogonal, in the sense that $|\cos(\varphi_{B-B',\beta})| \leq c$, where $0 \leq \varphi_{v,w} \leq \pi$ denotes the angle between two non-zero vectors $v, w \in \mathbb{R}^2$. Let s', s'' be the two straight lines through B satisfying

$$|\cos(\varphi_{s',\beta})| = |\cos(\varphi_{s'',\beta})| = c.$$

Let D be the further intersection between the circle $\sqrt{m}\mathcal{S}^1$ and s', meaning $\sqrt{m}\mathcal{S}^1 \cap s' = \{B, D\}$. Likewise, let E be the further intersection between $\sqrt{m}\mathcal{S}^1$ and s'', meaning $\sqrt{m}\mathcal{S}^1 \cap s'' = \{B, E\}$. Note that possibly one of the lines s', s'',

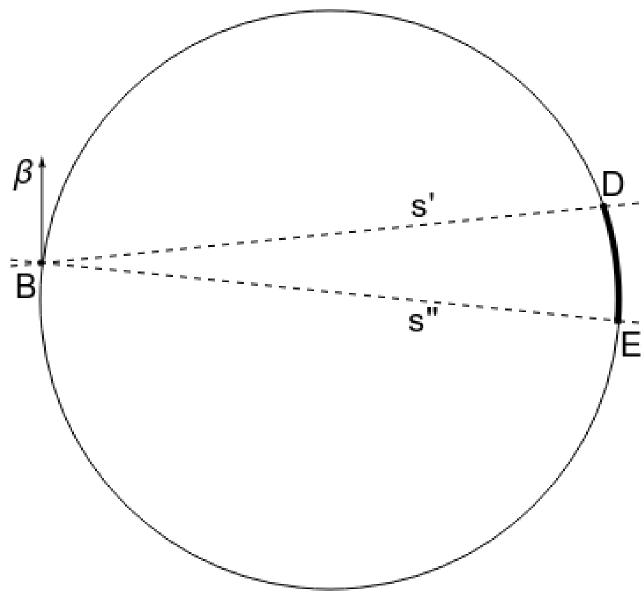

Figure 3.4.1: Points lying on a short arc - first case.

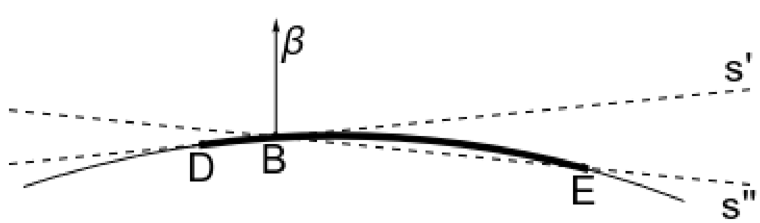

Figure 3.4.2: Points lying on a short arc - second case.

say s'', is tangent to the circle $\sqrt{m}\mathcal{S}^1$, in which case $E = B$. We have (see figures 3.4.1 and 3.4.2) $B' \in \overset{\frown}{DE}$ and we want to show $\overset{\frown}{DE} = (4c + O(c^3))\sqrt{m}$.

By the expansion
$$\arccos(c) = \frac{\pi}{2} - c + O(c^3)$$
we have
$$\varphi_{s',\beta} = \varphi_{s'',\beta} = \frac{\pi}{2} - c + O(c^3), \qquad \varphi_{s',s''} = \pi - \varphi_{s',\beta} - \varphi_{s'',\beta} = 2c + O(c^3).$$
Let D', D'' be points on s' on opposite sides of B, and E', E'' be points on s'' on opposite sides of B, so that: $\overline{BD'} = \overline{BD''} = \overline{BE'} = \overline{BE''} = 3\sqrt{m}$, D lies on s' between B and D', and $\widehat{D'BE'} = \varphi_{s',s''} = 2c + O(c^3)$. There are three cases:

- In case E lies on s'' between B and E' (as in figure 3.4.1), we have
$$\overset{\frown}{DE} = \widehat{DOE} \cdot \sqrt{m} = 2\widehat{D'BE'} \cdot \sqrt{m} = (4c + O(c^3))\sqrt{m}$$
where we have denoted O the origin, centre of $\sqrt{m}\mathcal{S}^1$.

- In case E lies on s'' between B and E'' (as in figure 3.4.2), then B lies on the arc $\overset{\frown}{DE}$ and we have
$$\overset{\frown}{DE} = (\widehat{DOB} + \widehat{EOB})\sqrt{m} = (2\widehat{DEB} + 2\widehat{EDB})\sqrt{m} = 2\widehat{D'BE'} \cdot \sqrt{m}$$
$$= (4c + O(c^3))\sqrt{m}.$$

- In case $E = B$, we write
$$\overset{\frown}{DE} = \overset{\frown}{DB} = \widehat{DOB} \cdot \sqrt{m} = 2\widehat{D'BE'} \cdot \sqrt{m} = (4c + O(c^3))\sqrt{m}.$$

$\square$

Proposition 3.4.2. *Let A_α be as in Definition 3.3.1, and recall that $\|\alpha\| = 1$. Assume that every arc on $\sqrt{m}\mathcal{S}^1$ of length J contains at most l lattice points. Then*
$$\frac{1}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \ll \left(\left(\frac{l}{J}\right)^4 \cdot \frac{m}{\mathcal{N}^4}\right)^{1/5} + \frac{l}{\mathcal{N}}.$$

Proof. Let $a \leq 2\sqrt{m}$ and c be positive parameters, such that $c \to 0$ as $m \to \infty$. We separate the sum over the following three ranges:

- first range: $\|\mu - \mu'\| \leq a$
- second range: $|\langle \mu - \mu', \alpha \rangle| \leq c\|\mu - \mu'\|$
- third range: $\|\mu - \mu'\| \geq a,\ |\langle \mu - \mu', \alpha \rangle| \geq c\|\mu - \mu'\|$.

We may now rewrite

$$\sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \leq \#\{(\mu, \mu') : \|\mu - \mu'\| \leq a\}$$
$$+ \#\{(\mu, \mu') : |\langle \mu - \mu', \alpha \rangle| \leq c\|\mu - \mu'\|\} + \sum_{\substack{\|\mu - \mu'\| \geq a \\ |\langle \mu - \mu', \alpha \rangle| \geq c\|\mu - \mu'\|}} \frac{1}{\langle \mu - \mu', \alpha \rangle^2}. \tag{3.4.2}$$

We will now show that there are few pairs of lattice points in the first two ranges, using bounds for lattice points on short arcs, together will Lemma 3.4.1. The contribution of the third range will be bounded pointwise.

First range: recall the notation $\sqrt{m}\mathcal{S}^1$ for the radius $\sqrt{m}$ circle. For a fixed lattice point μ, all μ' satisfying $\|\mu - \mu'\| \leq a$ must lie on a disc centred at μ with radius a; the intersection of this disc with $\sqrt{m}\mathcal{S}^1$ is an arc on $\sqrt{m}\mathcal{S}^1$ of length $\sim a$ around μ. To bound (from above) the number of μ' on this arc, we partition it into small arcs of length J: there are $\ll 1 + \frac{a}{J}$ small arcs, and by the assumptions of Proposition 3.4.2 each contains at most l lattice points. Therefore,

$$\#\{(\mu, \mu') : \|\mu - \mu'\| \leq a\} = O\left(\frac{a}{J} \cdot l \cdot \mathcal{N}\right) + O(l \cdot \mathcal{N}). \tag{3.4.3}$$

Second range: fix a lattice point μ and apply Lemma 3.4.1 with $\beta = \alpha$. Then all μ' satisfying $|\langle \mu - \mu', \alpha \rangle| \leq c\|\mu - \mu'\|$ must lie on an arc of length $(4c + O(c^3))\sqrt{m}$ on the circle $\sqrt{m}\mathcal{S}^1$. Partition this arc into small arcs of length

J: there are $\ll 1+\frac{4c\sqrt{m}}{J}$ small arcs, and each contains at most l lattice points. It follows that

$$\#\{(\mu,\mu'):|\langle\mu-\mu',\alpha\rangle|\leq c\|\mu-\mu'\|\}=O\left(\frac{c\sqrt{m}}{J}\cdot l\cdot\mathcal{N}\right)+O(l\cdot\mathcal{N}). \quad (3.4.4)$$

Third range. Here we have $\|\mu-\mu'\|\geq a$ and $|\langle\mu-\mu',\alpha\rangle|\geq c\|\mu-\mu'\|$, therefore

$$\sum\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\leq\sum\frac{1}{\|\mu-\mu'\|^2c^2}\leq\sum\frac{1}{a^2c^2}\leq\frac{\mathcal{N}^2}{a^2c^2}. \quad (3.4.5)$$

Substituting (3.4.3), (3.4.4) and (3.4.5) into (3.4.2), we obtain

$$\sum_{A_\alpha}\min\left(1,\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right) = O\left(\frac{a}{J}\cdot l\cdot\mathcal{N}\right)+O\left(\frac{c\sqrt{m}}{J}\cdot l\cdot\mathcal{N}\right)+O(l\cdot\mathcal{N})+O\left(\frac{\mathcal{N}^2}{a^2c^2}\right).$$

The optimal choices for the parameters are

$$a=c\sqrt{m}=\left(\frac{J}{l}\right)^{1/5}\cdot\mathcal{N}^{1/5}\cdot m^{1/5},$$

and it follows that

$$\frac{1}{\mathcal{N}^2}\cdot\sum_{A_\alpha}\min\left(1,\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right)\ll\left(\frac{l}{J}\right)^{4/5}\cdot\frac{m^{1/5}}{\mathcal{N}^{4/5}}+\frac{l}{\mathcal{N}}.$$

□

Proof of Theorems 1.2.6, 1.2.8 and 1.2.9

Corollary 3.4.3. *We have unconditionally*

$$\frac{1}{\mathcal{N}^2}\cdot\sum_{A_\alpha}\min\left(1,\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right)\ll\left(\frac{\log m}{\mathcal{N}}\right)^{4/5}+\frac{\log m}{\mathcal{N}}.$$

Proof. By Proposition 2.2.6, we may take $J = (\sqrt{m})^{1/2}$ and $l = O(\log(m))$ unconditionally in Proposition 3.4.2. $\square$

Proof of Theorem 1.2.6. Apply Proposition 3.3.2, yielding (3.3.5); by Corollary 3.4.3, we have

$$\mathrm{Var}(\mathcal{Z}) \ll \frac{m}{\mathcal{N}} + m \cdot \left(\frac{\log m}{\mathcal{N}}\right)^{4/5} + m \cdot \frac{\log m}{\mathcal{N}} \ll m \cdot \left(\frac{\log m}{\mathcal{N}}\right)^{4/5} \tag{3.4.6}$$

where we have assumed $\log m = o(\mathcal{N})$. $\square$

Corollary 3.4.4. *Assume Conjecture 1.2.7. Then*

$$\frac{1}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \ll \frac{1}{\mathcal{N}}.$$

Proof. By Conjecture 1.2.7, for some $\epsilon > 0$, we may take $J = (\sqrt{m})^{1/2+\epsilon}$ and $l = O(1)$ in Proposition 3.4.2:

$$\frac{1}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \ll \left(\left(\frac{1}{m^{\frac{1}{4}+\frac{\epsilon}{2}}}\right)^4 \cdot \frac{m}{\mathcal{N}^4}\right)^{1/5} + \frac{1}{\mathcal{N}} \ll \frac{1}{\mathcal{N}},$$

where the latter inequality follows from (1.2.8). $\square$

Proof of Theorem 1.2.8. Apply Proposition 3.3.2, yielding (3.3.5); by Corollary 3.4.4,

$$\mathrm{Var}(\mathcal{Z}) \ll \frac{m}{\mathcal{N}}.$$

$\square$

Corollary 3.4.5. *Let $\{m\} \subseteq S$ be a sequence satisfying*

$$\min_{\mu \neq \mu' \in \mathcal{E}_m} \|\mu - \mu'\| > (\sqrt{m})^{1-\epsilon}$$

for some $0 < \epsilon < \frac{1}{2}$ and sufficiently big m. Then

$$\frac{1}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \ll \frac{1}{\mathcal{N}}.$$

Proof. By the assumptions of Corollary 3.4.5, we have that on the circle $\sqrt{m}\mathcal{S}^1$ on any arc of length $< (\sqrt{m})^{1-\epsilon}$ there is at most one lattice point. Therefore, we may take $J = (\sqrt{m})^{1-\epsilon}$ and $l = 1$ in Proposition 3.4.2, yielding

$$\frac{1}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \ll \left(\left(\frac{1}{m^{\frac{1}{2}-\frac{\epsilon}{2}}}\right)^4 \cdot \frac{m}{\mathcal{N}^4}\right)^{1/5} + \frac{1}{\mathcal{N}} \ll \frac{1}{\mathcal{N}},$$

where the latter inequality follows from (1.2.8). □

Proof of Theorem 1.2.9. Apply Proposition 3.3.2, yielding (3.3.5); by Corollary 3.4.5, we have

$$\mathrm{Var}(\mathcal{Z}) \ll \frac{m}{\mathcal{N}}.$$

□

Chapter 4

Nodal intersections in 3D

The present chapter incorporates the publication [52]. We will prove Theorems 1.3.2, 1.3.3 and 1.3.5.

4.1 Outline

Recall that

$$\mathcal{E} = \mathcal{E}^{(3)} = \{\mu \in \mathbb{Z}^3 : \|\mu\|^2 = m\}$$

is the set of lattice points lying on the sphere of radius $\sqrt{m}$, and $\mathcal{N}^{(3)} = |\mathcal{E}^{(3)}|$ is their number. We work with the ensemble of arithmetic random waves (1.3.3)

$$F^{(3)}(x) = \frac{1}{\sqrt{\mathcal{N}^{(3)}}} \sum_{(\mu^{(1)},\mu^{(2)},\mu^{(3)})\in\mathcal{E}} a_\mu e^{2\pi i\langle\mu,x\rangle}, \tag{4.1.1}$$

defined on the three-dimensional flat torus $\mathbb{T}^3 := \mathbb{R}^3/\mathbb{Z}^3$. Given the toral straight line $\mathcal{C}$ (1.3.8)

$$\mathcal{C} : \gamma(t) = t(\alpha_1, \alpha_2, \alpha_3), \quad 0 \leq t \leq L, \quad \alpha \in \mathbb{R}^3, \quad \|\alpha\| = 1,$$

we wish to study the number of nodal intersections (1.3.4)

$$\mathcal{Z} = \mathcal{Z}_m^{(3)}(F) := |\{x \in \mathbb{T}^3 : F(x) = 0\} \cap \mathcal{C}|, \tag{4.1.2}$$

as $m \to \infty$.

In section 4.2, following Rudnick-Wigman-Yesha's work for generic curves [62], and similarly to the two-dimensional case of this problem (section 3.2), we count the nodal intersections (4.1.2) by the zeros of f (2.4.3)

$$f(t) := F(\gamma(t)) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{\mu \in \mathcal{E}} a_\mu e^{2\pi i \langle \mu, \gamma(t) \rangle}, \tag{4.1.3}$$

the restriction of F to the line $\mathcal{C}$. We shall again appeal to the approximate Kac-Rice formula of Rudnick, Wigman and Yesha (see Proposition 3.2.1), which bounds the nodal intersections variance using the second moment of the covariance function r (2.4.4)

$$r(t_1, t_2) = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i \langle \mu, \gamma(t_1) - \gamma(t_2) \rangle} \tag{4.1.4}$$

of f and a couple of its derivatives.

Let us highlight the marked differences between the straight line and generic curve settings. If $\mathcal{C}$ is a straight line segment, the covariance function has the special form (2.4.6)

$$r(t_1, t_2) = \frac{1}{\mathcal{N}} \sum_{\mu \in \mathcal{E}} e^{2\pi i (t_1 - t_2) \langle \mu, \alpha \rangle},$$

so that the process f is stationary. This leads to a different method from [62] of controlling the second moment of r, and specifically the quantity

$$\sum_{\substack{\mu, \mu' \in \mathcal{E} \\ \mu \neq \mu'}} \left| \int_0^L e^{2\pi i \langle \mu - \mu', \gamma(t) \rangle} dt \right|^2. \tag{4.1.5}$$

Indeed, for curves with nowhere vanishing curvature, we have an oscillatory integral in (4.1.5), thus Van der Corput's lemma [62, section 3] applies and reduces the problem to bounding the following summations over the lattice points:

$$\sum_{\substack{\mu,\mu'\in\mathcal{E}\\ \mu\neq\mu'}} \frac{1}{|\mu-\mu'|^j} \qquad \text{for } j=2/3,1.$$

For straight lines, we may directly establish the following bound for the integral in (4.1.5): if $\langle\mu-\mu',\alpha\rangle\neq 0$, then (cf. (4.3.2))

$$\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 \ll \min\left(1,\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right).$$

Thus, we need to understand the summation

$$\sum_{\substack{\mu,\mu'\in\mathcal{E}\\ \langle\mu-\mu',\alpha\rangle\neq 0}} \frac{1}{\langle\mu-\mu',\alpha\rangle^2} \tag{4.1.6}$$

where α is the direction of our straight line.

In section 4.3, we bound (4.1.6) for α rational, and thus complete the proof of Theorem 1.3.2. For α irrational, (4.1.6) may be controlled by counting lattice points in certain regions of the sphere $R\mathcal{S}^2$. To this end, in section 4.4, we recall results about lattice points on spheres and in spherical caps. Moreover, in sections 4.4 and 4.5 we prove bounds for the number of lattice points lying in regions of $R\mathcal{S}^2$ delimited by two parallel planes (i.e., *"spherical segments"*; cf. Definition 4.4.3); some of these bounds rely on Diophantine approximation. Theorems 1.3.3 (A), 1.3.3 (B) and 1.3.5 are thus established in sections 4.6, 4.7 and 4.8 respectively.

4.2 A Kac-Rice type bound

The following discussion is similar to the two-dimensional case (section 3.2). Recall that the arithmetic random wave (4.1.1) is a stationary centred Gaussian field on the torus (recall section 2.4.2). For now we assume $\mathcal{C}$ to be a smooth toral curve (allowing but not imposing it to be a straight line segment), with arc-length parametrisation given by $\gamma(t) : [0, L] \to \mathbb{T}^3$. The nodal intersections $\mathcal{Z}^{(3)}$ (4.1.2) are counted by the zeros of the process $f = F(\gamma)$ (4.1.3). The moments of $\mathcal{Z}$ may be studied via the Kac-Rice formulas of section 2.4.3. Since f is unit variance, the non-degeneracy condition of Theorem 2.4.8 is automatically satisfied when $j = 1$: therefore,

$$\mathbb{E}[\mathcal{Z}] = \int_0^L K_1(t)dt. \tag{4.2.1}$$

Rudnick, Wigman and Yesha [62, Lemma 2.3] found that, on the d-dimensional torus $\mathbb{T}^d$, $K_1(t) \equiv \frac{2}{\sqrt{d}}\sqrt{m}$, and hence by (4.2.1), they computed the expected intersection number to be $L\frac{2}{\sqrt{3}} \cdot \sqrt{m}$ (1.3.6).

For the nodal intersections variance, similarly to the two-dimensional case, the non-degeneracy hypothesis of Theorem 2.4.8 is equivalent to the covariance function (4.1.4) of the process (which also verifies $|r| \leq 1$) satisfying $r(t_1, t_2) \neq \pm 1$ for all $t_1 \neq t_2$. Since this condition may fail in our setting, we shall again invoke the approximate Kac-Rice formula of Rudnick-Wigman-Yesha (see Proposition 3.2.1).

4.3 Rational lines: proof of Theorem 1.3.2

In this section, we prove Theorem 1.3.2. Recall the notation

$$\mathcal{E}_m^{(3)} := \{(\mu^{(1)}, \mu^{(2)}, \mu^{(3)}) \in \mathbb{Z}^3 : (\mu^{(1)})^2 + (\mu^{(2)})^2 + (\mu^{(3)})^2 = m\}.$$

for the lattice point set and

$$\mathcal{N} = |\mathcal{E}| = r_3(m)$$

for its cardinality. Also recall that

$$R := \sqrt{m},$$

and $R\mathcal{S}^{d-1}$ is the $d-1$-dimensional sphere of radius R. From this point on, assume $\mathcal{C} \subset \mathbb{T}^3$ to be a straight line segment as in (1.3.8). Proposition 3.2.1 holds for all smooth curves $\mathcal{C}$, and in particular for straight line segments. We may further reduce our problem to bounding a sum over the lattice points.

Lemma 4.3.1. *If $\mathcal{C} \subset \mathbb{T}^3$ is a straight line segment as in* (1.3.8)*, then we have*

$$\mathfrak{R}_2(m) \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2,$$

with $\mathfrak{R}_2(m)$ as in (3.2.4)*.*

The proof of Lemma 4.3.1 is very similar to the proof of two-dimensional analogue Lemma A.1.1, and is thus omitted.

Proposition 4.3.2. *If $\mathcal{C} \subset \mathbb{T}^3$ is a straight line segment as in* (1.3.8)*, then we have*

$$Var\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2. \tag{4.3.1}$$

Proof. By Proposition 3.2.1 and Lemma 4.3.1,

$$\text{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \mathfrak{R}_2(m) \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2.$$

□

We remark that, if $\langle \mu-\mu',\alpha\rangle \neq 0$, then (cf. (A.1.7) and (A.1.8))

$$\left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2 \ll \min\left(1, \frac{1}{\langle \mu-\mu',\alpha\rangle^2}\right). \tag{4.3.2}$$

It then remains to bound the summation (4.1.6). We do this first for α rational. Recall Definition 1.3.1: $\kappa(R)$ denotes the maximal number of lattice points in the intersection of $R\mathcal{S}^2$ and a plane.

Lemma 4.3.3. *For $\alpha \in \mathbb{R}^3$,*

$$\#\{(\mu,\mu') \in \mathcal{E}^2 : \ \langle \mu-\mu', \alpha\rangle = 0\} \leq \mathcal{N} \cdot \kappa(\sqrt{m}). \tag{4.3.3}$$

Proof. We rewrite the LHS of (4.3.3) as

$$\sum_{\mu\in\mathcal{E}} \#\{\mu' : \ \langle \mu-\mu', \alpha\rangle = 0\} = \sum_{\mu\in\mathcal{E}} \#\{\mu' : \ \langle \mu', \alpha\rangle = \langle \mu, \alpha\rangle\}.$$

This means μ' belongs to the plane

$$\langle \alpha, (x,y,z)\rangle = \xi, \tag{4.3.4}$$

where $\xi := \langle \mu, \alpha\rangle \in \mathbb{R}$. By Definition 1.3.1, (4.3.4) has at most $\kappa(\sqrt{m})$ solutions $(x,y,z) \in \mathcal{E}$. Therefore,

$$\sum_{\mu\in\mathcal{E}} \#\{\mu' : \ \langle \mu', \alpha\rangle = \langle \mu, \alpha\rangle\} \leq \sum_{\mu\in\mathcal{E}} \kappa(\sqrt{m}) = \mathcal{N} \cdot \kappa(\sqrt{m}).$$

□

Lemma 4.3.4. *For rational vectors α,*

$$\sum_{\langle \mu-\mu',\alpha\rangle\neq 0} \frac{1}{\langle \mu-\mu', \alpha\rangle^2} \ll_\alpha \mathcal{N} \cdot \kappa(\sqrt{m}).$$

Proof. Up to multiplication by a constant, α has integer components:

$$(\alpha_1,\alpha_2,\alpha_3) = \alpha_1 \cdot \left(1, \frac{\alpha_2}{\alpha_1}, \frac{\alpha_3}{\alpha_1}\right) = \alpha_1 \cdot \left(1, \frac{p}{q}, \frac{r}{s}\right)$$

where $p,q,r,s \in \mathbb{Z}$ and $q,s \neq 0$. Then

$$(\alpha_1,\alpha_2,\alpha_3) = \alpha_1 \cdot \frac{1}{q} \cdot \frac{1}{s} \cdot (qs, ps, qr) = \frac{\alpha_1}{qs} \cdot (a,b,c)$$

with $a,b,c \in \mathbb{Z}$. Therefore,

$$\begin{aligned}
\sum_{\langle \mu-\mu',\alpha\rangle\neq 0} \frac{1}{\langle \mu-\mu', \alpha\rangle^2} &= \sum_{\langle \mu-\mu',\alpha\rangle\neq 0} \frac{1}{(\frac{\alpha_1}{qs})^2 \cdot \langle \mu-\mu', (a,b,c)\rangle^2} \\
\ll_\alpha \sum_{\langle \mu-\mu',\alpha\rangle\neq 0} \frac{1}{\langle \mu-\mu', (a,b,c)\rangle^2} &= \sum_{\mu} \sum_{k\neq 0} \sum_{\substack{\mu' \\ \langle \mu-\mu',(a,b,c)\rangle = k}} \frac{1}{k^2} \\
&= \sum_{\mu} \sum_{k\neq 0} \frac{1}{k^2} \cdot \#\{\mu' : \langle (a,b,c), \mu'\rangle = \xi = \xi(\mu,k) \in \mathbb{Z}\}.
\end{aligned}$$

As μ' belongs to the plane $ax+by+cz=\xi$, we have at most $\kappa(\sqrt{m})$ solutions. Therefore,

$$\sum_{\langle\mu-\mu',\alpha\rangle\neq 0}\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\ll_\alpha\sum_{\mu}\sum_{k\neq 0}\frac{\kappa(\sqrt{m})}{k^2}\ll\kappa(\sqrt{m})\sum_{\mu}1=\mathcal{N}\cdot\kappa(\sqrt{m}).$$

□

Proof of Theorem 1.3.2. By Proposition 4.3.2, we have (4.3.1). We separate the summation on the RHS of (4.3.1) and apply (4.3.2):

$$\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right)\ll\frac{1}{\mathcal{N}^2}\left(\sum_{\langle\mu-\mu',\alpha\rangle=0}1+\sum_{\langle\mu-\mu',\alpha\rangle\neq 0}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2\right)\tag{4.3.5}$$

$$\ll\frac{1}{\mathcal{N}^2}\left(\#\{(\mu,\mu')\in\mathcal{E}^2:\ \langle\mu-\mu',\alpha\rangle=0\}+\sum_{\langle\mu-\mu',\alpha\rangle\neq 0}\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right).$$

Both summands on the RHS of (4.3.5) are $\ll\mathcal{N}\cdot\kappa(\sqrt{m})$, by Lemmas 4.3.3 and 4.3.4 respectively. □

As mentioned in section 1.3, Theorem 1.3.2 loses by the factor $\kappa(\sqrt{m})$ with respect to the 2-dimensional case (Theorem 1.2.5): for on the radius $\sqrt{m}$ circle, the maximal number of lattice points on the same hyperplane (line) is $\kappa_2(\sqrt{m})\leq 2$; on the radius $\sqrt{m}$ sphere, the maximal number of lattice points on the same hyperplane (plane) is (1.3.9)

$$\kappa_3(\sqrt{m})\ll(\sqrt{m})^\epsilon.\tag{4.3.6}$$

4.4 Lattice points in specific regions of the sphere

We now turn to the case of intersections with irrational lines; we will need upper bounds for the number of lattice points in specific regions of the sphere $R\mathcal{S}^2=\sqrt{m}\mathcal{S}^2$.

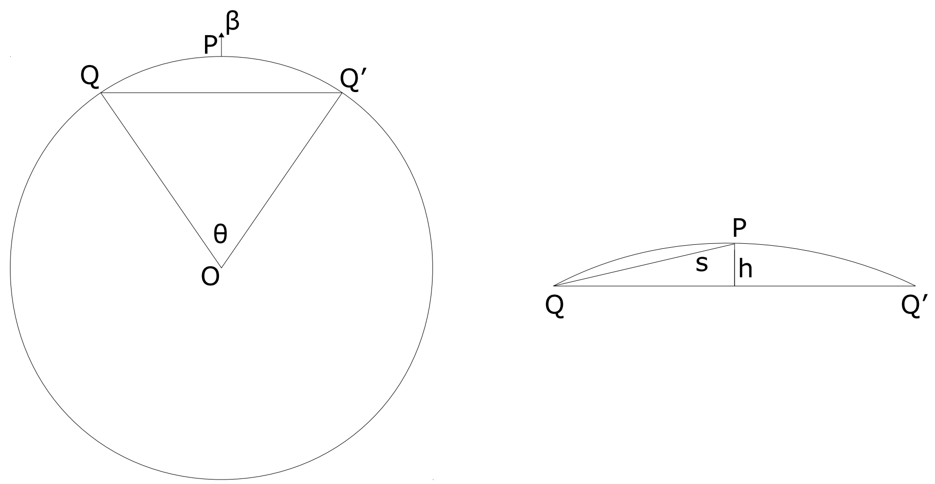

Figure 4.4.1: A spherical cap; projection on the plane containing P, Q, Q'.

Lattice points in spherical caps.

Definition 4.4.1. Given a sphere Σ in $\mathbb{R}^3$, with centre O and radius R, and a point $P \in \Sigma$, we define the **spherical cap** T centred at P to be the intersection of Σ with the ball $B_s(P)$ of radius s centred at P. We will call s the **radius of the cap**, and the unit vector $\beta := \frac{\overrightarrow{OP}}{R}$ the **direction** of T (see figure 4.4.1).

The intersection of Σ with the boundary of $B_s(P)$ is a circle; it will be called the **base** of T, and the **radius of the base** will be denoted k. Let Q, Q' be two points on the base which are diametrically opposite (note $\overline{PQ} = \overline{PQ'} = s$): we define the **opening angle** of T to be $\theta = \widehat{QOQ'}$. The **height** h of T is the distance between the point P and the disc base. Equivalently, T may be defined as the region of the sphere Σ delimited by a plane; the intersection of this plane with Σ is the base of T.

If s, h, k and θ denote the radius, height, radius of the base, and opening angle of T respectively, then we have $0 \leq s \leq 2R$, $0 \leq h \leq 2R$, $0 \leq k \leq R$ and

$0 \leq \theta \leq \pi$. Furthermore, geometric considerations give the relations

$$k^2 + h^2 = s^2 = 2Rh \tag{4.4.1}$$

and

$$s = 2R\sin(\theta/4). \tag{4.4.2}$$

From (4.4.1) and (4.4.2) we deduce

$$\theta = 4\arcsin\left(\sqrt{h/2R}\right). \tag{4.4.3}$$

We shall denote

$$\chi(R, s) = \max_T \#\{\mu \in \mathbb{Z}^3 \cap T\} \tag{4.4.4}$$

the maximal number of lattice points belonging to a spherical cap $T \subset R\mathcal{S}^2$ of radius s: (4.4.4) is a 3-dimensional analogue of lattice points on short arcs of a circle (section 2.2.2).

Lemma 4.4.2 (Bourgain and Rudnick [10, Lemma 2.1])**.** *We have for all $\epsilon > 0$,*

$$\chi(R, s) \ll R^\epsilon \left(1 + \frac{s^2}{R^{1/2}}\right)$$

as $R \to \infty$.

Compare this result with Conjecture 1.3.4.

Spherical segments: definitions and notation.

Definition 4.4.3. Given a sphere Σ in $\mathbb{R}^3$, and two parallel planes Π_1, Π_2 which both have non-empty intersection with Σ, we call **spherical segment** S the region of the sphere delimited by Π_1, Π_2. The two **bases** of S are the circles $\mathcal{B}_1 = \Sigma \cap \Pi_1$ and $\mathcal{B}_2 = \Sigma \cap \Pi_2$, the latter being the larger of the two.

It will be convenient to always assume a spherical segment S to be contained in a hemisphere. If this is not the case, then there exist two spherical segments S_1 and S_2, each contained in a hemisphere, such that $S_1 \cup S_2 = S$, $S_1 \cap S_2 = \mathcal{B}$ with $\mathcal{B}$ a great circle of the sphere. Therefore, a property of S may be derived by working on S_1 and S_2.

Definition 4.4.4. Given a spherical segment S with same notation as in Definition 4.4.3, we define its **height** h to be the distance between Π_1 and Π_2. We will denote k the **radius of the larger base** $\mathcal{B}_2$. Moreover, let Γ be a great circle of the sphere Σ, lying on a plane perpendicular to Π_1 and Π_2. Denote $\{A, B\} := \mathcal{B}_1 \cap \Gamma$, $\{C, D\} := \mathcal{B}_2 \cap \Gamma$ and call O the centre of the sphere. We define the **opening angle** of S to be $\theta = \widehat{AOC} + \widehat{BOD} = 2 \cdot \widehat{AOC}$.

Consider the special case when the spherical segment is a cap, i.e. $\mathcal{B}_1$ is a point. With the notation of Definition 4.4.4, since the points A and B coincide, we get $\theta = \widehat{AOC} + \widehat{BOD} = \widehat{COD}$, which is consistent with the definition of the opening angle for a spherical cap (see Definition 4.4.1). Note that any two of h, k, θ completely determine S (recall we are assuming the segment to be contained in a hemisphere). We always have $0 \leq h \leq R$, $0 \leq k \leq R$ and $0 \leq \theta \leq \pi$. We may also regard a spherical segment S as the difference set of two spherical caps T_1 and T_2:

$$S = T_2 \setminus T_1.$$

We will need the following lemma later; see appendix B for the proof.

Lemma 4.4.5. *Given a spherical segment $S \subset R\mathcal{S}^2$ of height $h(R)$, radius of larger base $k(R)$ and opening angle $\theta(R)$, we have*

$$k\theta \ll h$$

as $R \to \infty$.

Lattice points in spherical segments: covering the segment with caps. We want to give an upper bound for the maximal number of lattice points belonging to a spherical segment S of the sphere $R\mathcal{S}^2$,

$$\psi = \psi(R, h, k, \theta) := \max_S \#\{\mu \in \mathbb{Z}^3 \cap S\}, \tag{4.4.5}$$

with h, k, θ as in Definition 4.4.4.

Proposition 4.4.6. *Let $S \subset R\mathcal{S}^2$ be a spherical segment of opening angle θ and radius of larger base k. Then for every real number $0 < \Omega < R$,*

$$\psi \leq \chi(R, (2\pi + 1/2)\Omega) \cdot \left\lceil \frac{k}{\Omega} \right\rceil \cdot \left\lceil \frac{R\theta}{\Omega} \right\rceil \tag{4.4.6}$$

with $\chi(R, \cdot)$ as in (4.4.4).

Proof. Given a real number $0 < \Omega < R$, we will partition S into regions $\mathcal{R}_{ij}$ (described below), and then cover each $\mathcal{R}_{ij}$ with a spherical cap of radius $(2\pi + 1/2)\Omega$. Therefore, ψ does not exceed the number of lattice points $\chi(R, (2\pi + 1/2)\Omega)$ in a cap, times the number of caps.

The partitioning is done as follows. Denote $\mathcal{B}_1, \mathcal{B}_2$ the two bases of S, lying on the parallel planes Π_1, Π_2 respectively; the larger base $\mathcal{B}_2$ has radius k. Consider a set of great semicircles

$$\left\{ \Gamma_i, 1 \leq i \leq \left\lceil \frac{k}{\Omega} \right\rceil \right\}$$

lying on planes all perpendicular to Π_1, Π_2, and chosen so that they partition the circle $\mathcal{B}_2$ into $\lceil k/\Omega \rceil$ identical arcs each of length

$$\delta := \frac{2\pi k}{\lceil k/\Omega \rceil} \leq 2\pi\Omega.$$

For $1 \leq i \leq \lceil k/\Omega \rceil$, the arcs $S \cap \Gamma_i$ have length $R\theta/2$. Moreover, let

$$\left\{ \Lambda_j, 1 \leq j \leq \left\lfloor \frac{R\theta}{\Omega} \right\rfloor \right\}$$

be a set of circles on $R\mathcal{S}^2$, all lying on planes parallel to Π_1, Π_2, that partition each arc $S \cap \Gamma_i$ into $\lceil R\theta/\Omega \rceil$ identical smaller arcs of length

$$\eta := \frac{R\theta}{2 \lceil R\theta/\Omega \rceil} \leq \frac{1}{2}\Omega.$$

Notice that the Γ_i's and Λ_j's partition S into

$$\left\lceil \frac{k}{\Omega} \right\rceil \cdot \left\lceil \frac{R\theta}{\Omega} \right\rceil \tag{4.4.7}$$

regions $\mathcal{R}_{ij} \subset R\mathcal{S}^2$. We now show that each $\mathcal{R}_{ij}$ may be covered by a spherical cap of radius $(2\pi + 1/2)\Omega$.

We will use the notation

$$\overset{\frown\Lambda}{AB}$$

for an arc of a circle Λ of the sphere $R\mathcal{S}^2$, of endpoints A and B. The arc $\overset{\frown\Lambda}{AB}$ is a geodesic if and only if Λ is a great circle of $R\mathcal{S}^2$. In this case, we will simply write $\overset{\frown}{AB}$. The region $\mathcal{R}_{ij}$ is delimited by four arcs:

$$\overset{\frown\Lambda_j}{AB} \subset \Lambda_j, \quad \overset{\frown}{BC} \subset \Gamma_i, \qquad \overset{\frown\Lambda_{j+1}}{CD} \subset \Lambda_{j+1}, \quad \overset{\frown}{AD} \subset \Gamma_{i+1}.$$

By the construction of the circles $\{\Gamma_i\}_i$ and $\{\Lambda_j\}_j$, we have the relations

$$\overset{\frown\Lambda_j}{AB} < \overset{\frown\Lambda_{j+1}}{CD} \leq \delta, \qquad \overset{\frown}{BC} = \overset{\frown}{AD} = \eta.$$

Given any point $P \in \mathcal{R}_{ij}$, we denote $\overline{AP}$ the euclidean distance between A and P. Let us show that $\overline{AP} \leq (2\pi + 1/2)\Omega$, so that $\mathcal{R}_{ij}$ may be covered by the spherical cap of radius $(2\pi + 1/2)\Omega$ centred at A. Let Λ_P be the circle on $R\mathcal{S}^2$ containing P and lying on a plane parallel to Π_1, Π_2. Let Q be the intersection between Λ_P and $\overset{\frown}{AD}$. The euclidean distance between A and P is less than the length of the geodesic $\overset{\frown}{AP}$, which, in turn, is less that the sum of the lengths of the geodesics $\overset{\frown}{AQ}$ and $\overset{\frown}{QP}$. Moreover, we have

$$\overset{\frown}{QP} \leq \overset{\frown\Lambda_P}{QP} \leq \overset{\frown\Lambda_{j+1}}{CD} \leq \delta \leq 2\pi\Omega \qquad \text{and} \qquad \overset{\frown}{AQ} \leq \overset{\frown}{AD} = \eta \leq \frac{1}{2}\Omega.$$

It follows that, as desired,

$$\overline{AP} < \overset{\frown}{AP} \leq \overset{\frown}{AQ} + \overset{\frown}{QP} \leq \left(2\pi + \frac{1}{2}\right)\Omega.$$

The total number of caps equals the number of regions (4.4.7); therefore,

$$\psi \leq \chi(R, (2\pi + 1/2)\Omega) \cdot \left\lceil \frac{k}{\Omega} \right\rceil \cdot \left\lceil \frac{R\theta}{\Omega} \right\rceil,$$

as claimed. $\square$

Corollary 4.4.7. *Let $S \subset R\mathcal{S}^2$ be a spherical segment of opening angle θ and radius of larger base k. Then for every real number $0 < \Omega < R$ and for every $\epsilon > 0$, we have unconditionally*

$$\psi \ll R^\epsilon \left(1 + \frac{\Omega^2}{R^{\frac{1}{2}}}\right) \cdot \left\lceil \frac{k}{\Omega} \right\rceil \cdot \left\lceil \frac{R\theta}{\Omega} \right\rceil . \tag{4.4.8}$$

Proof. By Lemma 4.4.2, we may unconditionally insert the bound

$$\chi(R, (2\pi + 1/2)\Omega) \ll R^\epsilon \left(1 + \frac{((2\pi + 1/2)\Omega)^2}{R^{1/2}}\right) \ll R^\epsilon \left(1 + \frac{\Omega^2}{R^{1/2}}\right)$$

into (4.4.6), obtaining (4.4.8). □

Corollary 4.4.8. *Assume Conjecture 1.3.4. Let $S \subset R\mathcal{S}^2$ be a spherical segment of height h and radius of larger base k. Then for every $\epsilon > 0$,*

$$\psi \ll R^\epsilon \cdot (R^{1/2} + h).$$

Proof. The opening angle of the spherical segment S shall be denoted θ. By Proposition 4.4.6, we have (4.4.6) for every real number $0 < \Omega < R$. By Conjecture 1.3.4, it follows that, for every $\epsilon > 0$,

$$\psi \ll R^\epsilon \cdot \left(1 + \frac{((2\pi + 1/2)\Omega)^2}{R}\right) \cdot \left(1 + \frac{k}{\Omega}\right) \cdot \left(1 + \frac{R\theta}{\Omega}\right).$$

We take $\Omega = R^{1/2}$, hence

$$\psi \ll R^\epsilon \cdot \left(1 + \frac{k}{R^{1/2}}\right) \cdot (1 + R^{1/2}\theta) = R^\epsilon \left(1 + \frac{k}{R^{1/2}} + R^{1/2}\theta + k\theta\right).$$

Since $0 \le k \le R$ and $0 \le \theta \le \pi$, we obtain

$$\psi \ll R^\epsilon (R^{1/2} + k\theta).$$

Finally, by Lemma 4.4.5, it follows that $k\theta \ll h$. □

4.5 Lattice points in spherical segments: Diophantine approximation

Recall the notation ψ (4.4.5) for the maximal number of lattice points lying on a spherical segment $S \subset R\mathcal{S}^2$ of height h, radius of larger base k, and opening angle θ. The goal of this section is to prove a bound for ψ which depends only on θ. Recall Definition 1.3.1 for $\kappa(R)$, and Definition 4.4.1 for the direction β of a spherical cap.

Definition 4.5.1. The **direction** of a spherical segment S is the unit vector $\beta = (\beta_1, \beta_2, \beta_3)$ which is the direction of the two spherical caps T_1, T_2 satisfying

$$S = T_2 \setminus T_1.$$

Proposition 4.5.2. *Let $S \subset R\mathcal{S}^2$ be a spherical segment of opening angle θ, radius of larger base k, and direction β, with $\frac{\beta_2}{\beta_1}, \frac{\beta_3}{\beta_1} \in \mathbb{R} \setminus \mathbb{Q}$. Then the number of lattice points lying on S satisfies*

$$\psi \ll \kappa(R)(1 + R \cdot \theta^{1/3})$$

for $\theta \to 0$, the implied constant being absolute.

The proof of this result will be given at the end of the present section, following some preparation. We will apply the ideas of [10, Lemma 2.3]: firstly, we shall consider a spherical cap T or segment S', containing S, and of direction a rational vector $a/\|a\|$, where a_1, a_2, a_3 are parameters. Thus

$$\psi \leq \#\{\text{lattice points in } T \text{ or } S'\}.$$

We will then have to work with a larger portion of the sphere; however, as the new cap or segment's direction is a rational vector, the 'slicing' method of [10] may be applied, yielding

$$\psi \ll \kappa(R) \cdot [1 + R\|a\|(\theta + \varphi)]$$

where $a = (a_1, a_2, a_3) \in \mathbb{Z}^3$ and φ is the angle between β and a. Finally, to minimise the quantity $\|a\|(\theta + \varphi)$, we will choose values for the parameters $a_1, a_2, a_3 \in \mathbb{Z}$ such that both $\|a\|$ and φ are small, applying Diophantine approximation. Let us commence this preparatory work.

To bound the number of lattice points in a spherical segment of direction a *rational vector*, we apply the 'slicing' method of [10, proof of Lemma 2.3]; see also Yesha [73, Lemma A.1].

Proposition 4.5.3. *Let $S \subset R\mathcal{S}^2$ be a spherical segment of height h, radius of larger base k, and direction a rational vector $b/\|b\|$, where $b \in \mathbb{Z}^3$. Then, for any $0 \leq h \leq R$,*

$$\psi \leq \kappa(R) \cdot (1 + \|(b_1, b_2, b_3)\| \cdot h). \tag{4.5.1}$$

In particular, $\forall \epsilon > 0$,

$$\psi \ll_b R^\epsilon \cdot (1 + h). \tag{4.5.2}$$

Proof. Since $b \in \mathbb{Z}^3$, then for all lattice points μ, we have $\langle b, \mu \rangle = n \in \mathbb{Z}$, hence each lattice point on S belongs to a plane

$$\langle (b_1, b_2, b_3), (x, y, z) \rangle = n \tag{4.5.3}$$

intersecting S. It follows that ψ is bounded by the number $\nu(h, b)$ of planes (4.5.3) intersecting S times the number of lattice points lying on each plane. Therefore, recalling Definition 1.3.1, we have

$$\psi \leq \nu(h, b) \cdot \kappa(R). \tag{4.5.4}$$

It remains to bound $\nu(h, b)$. We claim that the minimal distance between two adjacent planes (4.5.3) both containing at least one lattice point is $\frac{n'}{\|(b_1,b_2,b_3)\|}$, n' being a positive integer. Indeed, consider two planes

$$\langle (b_1, b_2, b_3), (x, y, z) \rangle = n \qquad \text{and} \qquad \langle (b_1, b_2, b_3), (x, y, z) \rangle = n + n',$$

each containing at least one lattice point, with n' positive and as small as possible. Fix any point P on the former of these two planes, and a point Q on the latter so that the line through P, Q is orthogonal to the planes. The sought distance is thus $\|Q - P\|$. We have

$$\begin{cases} b_1 x_P + b_2 y_P + b_3 z_P = n & (4.5.5) \\ b_1 x_Q + b_2 y_Q + b_3 z_Q = n + n' & (4.5.6) \\ Q = P + \lambda(b_1, b_2, b_3), & (4.5.7) \end{cases}$$

which yields $\|Q - P\| = \|\lambda \cdot (b_1, b_2, b_3)\|$, with λ to be determined. By subtracting (4.5.5) from (4.5.6):

$$b_1(x_Q - x_P) + b_2(y_Q - y_P) + b_3(z_Q - z_P) = n'$$

i.e.,

$$\langle (b_1, b_2, b_3), Q - P \rangle = n'. \tag{4.5.8}$$

Inserting (4.5.7) into (4.5.8) yields

$$\langle (b_1, b_2, b_3), \lambda(b_1, b_2, b_3) \rangle = n' \Rightarrow \lambda \cdot \|(b_1, b_2, b_3)\|^2 = n' \Rightarrow \lambda = \frac{n'}{\|(b_1, b_2, b_3)\|^2}$$
$$\Rightarrow \|Q - P\| = \|\lambda(b_1, b_2, b_3)\| = \frac{n'}{\|(b_1, b_2, b_3)\|}.$$

As the height of the segment is h, we get

$$\nu(h, b) \leq 1 + \frac{h}{\|Q - P\|} = 1 + \|(b_1, b_2, b_3)\| \cdot \frac{h}{n'}.$$

Since $n' \geq 1$, it follows that

$$\nu(h, b) \leq 1 + \|(b_1, b_2, b_3)\| \cdot h$$

which together with (4.5.4) implies (4.5.1). In particular, recalling (4.3.6), we get (4.5.2). $\square$

The proof of the following lemma may be found in appendix B.

Lemma 4.5.4. *Let $S \subset R\mathcal{S}^2$ be a spherical segment of opening angle θ, radius of larger base k, and direction the unit vector β. For every non-zero $a = (a_1, a_2, a_3) \in \mathbb{Z}^3$, the maximal number of lattice points lying on S satisfies*

$$\psi \ll \kappa(R) \cdot [1 + R\|a\|(\theta + \varphi)] \tag{4.5.9}$$

where φ is the angle between β and a, and the implied constant is absolute.

Lemma 4.5.5. *Let v, w be two non-zero vectors of $\mathbb{R}^n$. Then*

$$\left\| \frac{v}{\|v\|} - \frac{w}{\|w\|} \right\| \leq 2\frac{\|v - w\|}{\|w\|}.$$

The proof of Lemma 4.5.5 is an application of the triangle inequality and is deferred to appendix B.

Lemma 4.5.6. *For all vectors $\alpha \in \mathbb{R}^3$ with $\frac{\alpha_2}{\alpha_1}, \frac{\alpha_3}{\alpha_1} \in \mathbb{R} \setminus \mathbb{Q}$ and $\|\alpha\| = 1$, and for all integers $H \geq 1$, there exists $a \in \mathbb{Z}^3$ satisfying*

$$\begin{cases} \|a\| \leq 3H^2 & (4.5.10) \\ \left\| \alpha - \dfrac{a}{\|a\|} \right\| < \dfrac{6\sqrt{2}}{\|a\|H}. & (4.5.11) \end{cases}$$

Proof of Lemma 4.5.6 assuming Lemma 4.5.5. As in [10, proof of Lemma 2.3], assume $|\alpha_1| = \max(|\alpha_1|, |\alpha_2|, |\alpha_3|)$. Take $\zeta_1 = \frac{\alpha_2}{\alpha_1}$, $\zeta_2 = \frac{\alpha_3}{\alpha_1}$ and a large integer H: by Proposition 2.1.3, there exist integers q, p_1, p_2 so that $1 \leq q \leq H^2$ and

$$\left| \frac{\alpha_2}{\alpha_1} - \frac{p_1}{q} \right|, \left| \frac{\alpha_3}{\alpha_1} - \frac{p_2}{q} \right| < \frac{1}{qH}.$$

We may assume $\alpha_1 > 0$ (in case $\alpha_1 < 0$, take $-\alpha$), and set $a = (a_1, a_2, a_3) := (q, p_1, p_2) \in \mathbb{Z}^3$. Then

$$\begin{aligned} |\alpha_1| = \max(|\alpha_1|, |\alpha_2|, |\alpha_3|) &\Rightarrow 0 \leq \left| \frac{\alpha_2}{\alpha_1} \right|, \left| \frac{\alpha_3}{\alpha_1} \right| \leq 1 \\ &\Rightarrow 0 \leq \left| \frac{p_1}{q} \right|, \left| \frac{p_2}{q} \right| \leq 1 + \frac{1}{qH} \leq 2 \Rightarrow |p_1|, |p_2| \leq 2q \\ \Rightarrow \|a\|^2 = q^2 + p_1^2 + p_2^2 \leq q^2 + 4q^2 + 4q^2 = 9q^2 &\Rightarrow \|a\| \leq 3q \leq 3H^2, \end{aligned}$$

and (4.5.10) is satisfied. We now turn to (4.5.11). We define the vector $d := \frac{\alpha_1}{q} \cdot a \in \mathbb{R}^3$, hence (as $\alpha_1 > 0$)

$$\frac{d}{\|d\|} = \frac{\frac{\alpha_1}{q} \cdot a}{\frac{|\alpha_1|}{|q|} \cdot \|a\|} = \frac{a}{\|a\|}.$$

We apply Lemma 4.5.5 with $w = \alpha$ and $v = d$, recalling that $\|\alpha\| = 1$:

$$\left\|\alpha - \frac{a}{\|a\|}\right\| = \left\|\frac{\alpha}{\|\alpha\|} - \frac{d}{\|d\|}\right\| \leq 2\frac{\|\alpha - d\|}{\|\alpha\|} = 2\|\alpha - d\|. \tag{4.5.12}$$

Moreover,

$$\begin{aligned}\|\alpha - d\| &= \left\|\alpha - \frac{\alpha_1}{q} \cdot (q, p_1, p_2)\right\| = \left\|\left(\alpha_1 - \frac{\alpha_1}{q} \cdot q, \alpha_2 - \frac{\alpha_1}{q} \cdot p_1, \alpha_3 - \frac{\alpha_1}{q} \cdot p_2\right)\right\| \\ &= |\alpha_1| \cdot \left\|\left(0, \frac{\alpha_2}{\alpha_1} - \frac{p_1}{q}, \frac{\alpha_3}{\alpha_1} - \frac{p_2}{q}\right)\right\| = |\alpha_1| \cdot \left(\left|\frac{\alpha_2}{\alpha_1} - \frac{p_1}{q}\right|^2 + \left|\frac{\alpha_3}{\alpha_1} - \frac{p_2}{q}\right|^2\right)^{1/2} \\ &< |\alpha_1| \cdot \left(2\left(\frac{1}{qH}\right)^2\right)^{1/2} = \sqrt{2} \cdot |\alpha_1| \cdot \frac{1}{qH} < \sqrt{2} \cdot \frac{1}{qH}.\end{aligned} \tag{4.5.13}$$

Since $\|a\| \leq 3q$, we have

$$\frac{1}{q} \leq \frac{3}{\|a\|}. \tag{4.5.14}$$

Combining (4.5.12), (4.5.13) and (4.5.14),

$$\left\|\alpha - \frac{a}{\|a\|}\right\| \leq 2\|\alpha - d\| < 2\sqrt{2} \cdot \frac{1}{qH} \leq 6\sqrt{2} \cdot \frac{1}{\|a\|H}$$

and (4.5.11) is satisfied. □

Proof of Proposition 4.5.2 assuming the preparatory results. By Lemma 4.5.4, we have for every non-zero $a = (a_1, a_2, a_3) \in \mathbb{Z}^3$,

$$\psi \ll \kappa(R) \cdot [1 + R\|a\|(\theta + \varphi)] \tag{4.5.15}$$

where φ is the angle between β and a. We are then looking for $a \in \mathbb{Z}^3$ which minimises the quantity $\|a\|(\theta + \varphi)$. We claim that

$$\varphi \sim \left\|\beta - \frac{a}{\|a\|}\right\| \quad \text{as } \theta \to 0 \tag{4.5.16}$$

(this will be shown at the end of the proof). By (4.5.15) and (4.5.16),

$$\psi \ll \kappa(R) \cdot \left[1 + R\left(\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\|\right)\right]. \tag{4.5.17}$$

It then suffices to bound

$$\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\|.$$

We want $a = (a_1, a_2, a_3)$ s.t. $\|a\|$ and $\|\beta - \frac{a}{\|a\|}\|$ are both small. We apply Lemma 4.5.6 with $\alpha = \beta$: for all integers $H \geq 1$, there exists $a = (a_1, a_2, a_3)$ so that

$$\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\| < 3H^2 \cdot \theta + \|a\| \frac{6\sqrt{2}}{\|a\|H} = 3H^2 \cdot \theta + \frac{6\sqrt{2}}{H}.$$

The tradeoff gives us the choice $H = \left\lfloor \left(\frac{2\sqrt{2}}{\theta}\right)^{1/3} \right\rfloor = \left\lfloor \frac{\sqrt{2}}{\theta^{1/3}} \right\rfloor$, hence

$$\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\| < 3\left(2\theta^{1/3} + 2\sqrt{2}\frac{1}{\lfloor \sqrt{2}/\theta^{1/3} \rfloor}\right) \ll \theta^{1/3}.$$

Inserting this bound into (4.5.17) yields the statement of Proposition 4.5.2:

$$\psi \ll \kappa(R) \cdot [1 + R \cdot \theta^{1/3}].$$

It remains to show (4.5.16). Consider the triangle of sides β, $\frac{a}{\|a\|}$ and $\beta - \frac{a}{\|a\|}$, of lengths $\|\beta\| = 1, \|a/\|a\|\| = 1$, and $x := \|\beta - \frac{a}{\|a\|}\|$ respectively. The angle opposite the side of length x is φ, hence $x = 2\sin(\varphi/2)$. If we show that $\varphi \to 0$ as $\theta \to 0$, it will imply $x = 2\sin(\varphi/2) \sim 2 \cdot \varphi/2 = \varphi$; it will suffice to show $x \to 0$ as $\theta \to 0$. By Lemma 4.5.6,

$$x \ll \frac{1}{\|a\|H}.$$

Since $\|a\| \geq 1$ and we chose $H = \left\lfloor \frac{\sqrt{2}}{\theta^{1/3}} \right\rfloor$, it follows that $x \ll \theta^{1/3} \to 0$ as $\theta \to 0$. $\square$

4.6 Proof of Theorem 1.3.3 (A)

The following is a three-dimensional analogue of Lemma 3.4.1. Recall the Definitions 4.4.1 of a spherical cap and 4.4.3 of a spherical segment.

Lemma 4.6.1. *Let $c = c(R) > 0$, with $c \to 0$ as $R \to \infty$. Fix a point $B \in R\mathcal{S}^2$, and let β be a unit vector. Then all points $B' \in R\mathcal{S}^2$ satisfying $|\langle B - B', \beta\rangle| \leq c\|B - B'\|$ lie: either on the same spherical segment S, of opening angle $\theta = 8c + O(c^3)$ and direction β; or on the same spherical cap, of radius $\ll cR$ and direction β, on $R\mathcal{S}^2$.*

Proof. The condition $|\langle B - B', \beta\rangle| \leq c\|B - B'\|$ means $B - B'$ and β are close to being orthogonal, in the sense that $|\cos(\varphi_{B-B',\beta})| \leq c$, where $0 \leq \varphi_{v,w} \leq \pi$ denotes the angle between two non-zero vectors $v, w \in \mathbb{R}^3$. Let $\{s_i\}_i$ be the set of straight lines through B satisfying

$$|\cos(\varphi_{s_i,\beta})| = c.$$

The lines $\{s_i\}_i$ are the generators of a cone with vertex B. Let $\mathcal{R}$ be the region of $\mathbb{R}^3$ delimited by this cone. We then have

$$\{B' \in \mathbb{R}^3 : |\cos(\varphi_{B-B',\beta})| \leq c\} = \mathbb{R}^3 \setminus \mathcal{R}.$$

It follows that

$$\{B' \in R\mathcal{S}^2 : |\cos(\varphi_{B-B',\beta})| \leq c\} = (\mathbb{R}^3 \setminus \mathcal{R}) \cap R\mathcal{S}^2 =: \mathcal{R}'.$$

We now show that $\mathcal{R}'$ is contained in either a spherical segment or cap. Let Π be the plane containing B and β (and thus also the origin O). The two lines belonging to the set $\{s_i\}_i$ and lying on Π will be denoted s', s''. Moreover, call D the further intersection between $R\mathcal{S}^2$ and s', meaning $R\mathcal{S}^2 \cap s' = \{B, D\}$. Likewise, call E the further intersection between $R\mathcal{S}^2$ and s'', meaning $R\mathcal{S}^2 \cap s'' = \{B, E\}$. Note that possibly one of the lines s', s'', say s'', is tangent to the sphere

$R\mathcal{S}^2$, in which case $E = B$. Let Π_1, Π_2 be planes orthogonal to β and through D, E respectively, and denote $\mathcal{B}_1 = R\mathcal{S}^2 \cap \Pi_1$, $\mathcal{B}_2 = R\mathcal{S}^2 \cap \Pi_2$. By the expansion

$$\arccos(c) = \frac{\pi}{2} - c + O(c^3)$$

we have

$$\varphi_{s',\beta} = \varphi_{s'',\beta} = \frac{\pi}{2} - c + O(c^3), \qquad \varphi_{s',s''} = \pi - \varphi_{s',\beta} - \varphi_{s'',\beta} = 2c + O(c^3).$$

Let D', D'' be points on s' on opposite sides of B, and E', E'' be points on s'' on opposite sides of B, so that: $\overline{BD'} = \overline{BD''} = \overline{BE'} = \overline{BE''} = 3R$, D lies on s' between B and D', and $\widehat{D'BE'} = \varphi_{s',s''} = 2c + O(c^3)$. There are two cases:

- In case E lies on s'' between B and E', we have $\mathcal{R}' \subset S$, where S is the spherical segment of bases $\mathcal{B}_1, \mathcal{B}_2$. The opening angle of S is

$$\theta = 2 \cdot \widehat{DOE} = 4 \cdot \widehat{D'BE'} = 8c + O(c^3).$$

- In case E lies on s'' between B and E'', or in case $E = B$, we have $\mathcal{R}' \subset T$, where T is the spherical cap of direction β and base either $\mathcal{B}_1$ or $\mathcal{B}_2$, whichever is the largest. Assume w.l.o.g. that the cap of base $\mathcal{B}_1 \ni D$ is the largest. Denoting $H = R\beta \in R\mathcal{S}^2$, the radius of T is

$$\overline{HD} \leq \overline{BD} = \widehat{DOB} \cdot R \leq 2 \cdot \widehat{D'BE'} \cdot R \ll cR.$$

□

Proof of Theorem 1.3.3 (A). Apply Proposition 4.3.2, yielding (4.3.1). Let $\rho = \rho(R)$ be a parameter such that $\rho \to 0$ as $R \to \infty$. Let us split the summation on the RHS of (4.3.1), applying (4.3.2):

$$\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{\mathcal{N}^2}\left[\sum_{|\langle\mu-\mu',\alpha\rangle| \leq \rho\cdot\|\mu-\mu'\|} 1 + \sum_{|\langle\mu-\mu',\alpha\rangle| \geq \rho\cdot\|\mu-\mu'\|} \frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right]. \tag{4.6.1}$$

To bound the first summation on the RHS of (4.6.1), we start by applying Lemma 4.6.1 with $c = \rho$, $B = \mu$ and $\beta = \alpha$: for fixed μ, the condition

$$|\langle \mu - \mu', \alpha \rangle| \leq \rho \cdot \|\mu - \mu'\|$$

means the lattice point μ' must lie on a spherical segment S_μ of opening angle $8\rho + O(\rho^3)$ and direction α, or on a spherical cap T_μ of radius $\ll \rho R$ and direction α, on $R\mathcal{S}^2$. It follows that

$$\begin{aligned}
&\#\{(\mu, \mu') : |\langle \mu - \mu', \alpha \rangle| \leq \rho \cdot \|\mu - \mu'\|\} \\
&= \sum_\mu \#\{\mu' : \mu' \in T_\mu\} + \sum_\mu \#\{\mu' : \mu' \in S_\mu\} \\
&\leq 2 \cdot \#\{(\mu, \mu') : \mu, \mu' \in T\} + \sum_\mu \#\{\mu' : \mu' \in S_\mu\}, \qquad (4.6.2)
\end{aligned}$$

where T is the spherical cap of radius $j\rho R$ (for some large enough $j \in \mathbb{R}^+$) and direction α. Recalling the notation (4.4.4), we may write

$$\#\{(\mu, \mu') : \mu, \mu' \in T\} = (\chi(R, j\rho R))^2.$$

If we assume $\rho = o(\frac{1}{R^{3/4}})$ (eventually we are going to choose $\rho = \frac{1}{R^{6/7}}$), we get

$$\#\{(\mu, \mu') : \mu, \mu' \in T\} \ll R^\epsilon \qquad (4.6.3)$$

by Lemma 4.4.2.

For each μ, the number of lattice points inside S_μ is bounded by the maximal number of lattice points ψ (recall (4.4.5)) in a spherical segment of opening angle $8\rho + O(\rho^3)$. We apply Proposition 4.5.2 with $\theta = 8\rho + O(\rho^3)$:

$$\sum_\mu \#\{\mu' : \mu' \in S_\mu\} \leq \sum_\mu \psi \ll \mathcal{N} \cdot \kappa(R)(1 + R \cdot \rho^{1/3}). \qquad (4.6.4)$$

By substituting (4.6.3) and (4.6.4) into (4.6.2), we get the following bound for the first summation on the RHS of (4.6.1):

$$\begin{aligned}
\#\{(\mu, \mu') : |\langle \mu - \mu', \alpha \rangle| \leq \rho \cdot \|\mu - \mu'\|\} &\ll R^\epsilon + \mathcal{N} \cdot \kappa(R)(1 + R \cdot \rho^{1/3}) \\
&\ll R^\epsilon \mathcal{N}(1 + R \cdot \rho^{1/3}), \qquad (4.6.5)
\end{aligned}$$

where we also used (4.3.6).

We now turn to the second summation on the RHS of (4.6.1). Let $\epsilon' > 0$ and apply Proposition 2.2.10 with $s = 2 - \epsilon'$:

$$\begin{aligned}\sum_{|\langle\mu-\mu',\alpha\rangle|\geq\rho\cdot\|\mu-\mu'\|}\frac{1}{\langle\mu-\mu',\alpha\rangle^2} &\leq \sum_{|\langle\mu-\mu',\alpha\rangle|\geq\rho\cdot\|\mu-\mu'\|}\frac{1}{\rho^2\|\mu-\mu'\|^2}\\ &\leq \frac{1}{\rho^2}\sum_{\mu\neq\mu'}\frac{1}{\|\mu-\mu'\|^{2-\epsilon'}} \sim \frac{\mathcal{N}^2}{\rho^2R^{2-\epsilon'}}. \end{aligned} \tag{4.6.6}$$

Inserting (4.6.5) and (4.6.6) into (4.6.1), and recalling (1.3.5), we deduce

$$\begin{aligned}\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) &\ll \frac{1}{\mathcal{N}^2}R^{\epsilon}\mathcal{N}\left(\left(1+R\cdot\rho^{1/3}\right)+\frac{\mathcal{N}}{\rho^2R^2}\right)\\ &\ll \frac{1}{\mathcal{N}^2}R^{\epsilon}\mathcal{N}\left(R\cdot\rho^{1/3}+\frac{1}{\rho^2R}\right). \end{aligned} \tag{4.6.7}$$

The optimal choice for the parameter is $\rho = \frac{1}{R^{6/7}}$, and it follows that

$$\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{\mathcal{N}\cdot R^{5/7+\epsilon}}{\mathcal{N}^2} \ll \frac{1}{m^{1/7-\epsilon}}.$$

□

As mentioned in the section 1.3, Theorem 1.3.3 (A) prescribes an unconditional bound for all energies m, whereas for the two-dimensional problem, an unconditional bound is only given for a *density one sequence* of energies (Theorem 1.2.9), and a bound for all m is given conditionally (Theorem 1.2.8). The reason for this is the significant difference between the total number of lattice points on a sphere and on a circle (compare (1.3.5) and (1.2.8)).

4.7 Proof of Theorem 1.3.3 (B)

For lines satisfying $\alpha_2/\alpha_1 \in \mathbb{Q}$ and $\alpha_3/\alpha_1 \in \mathbb{R}\setminus\mathbb{Q}$, we may unconditionally improve our bound for the variance of nodal intersections (Theorem 1.3.3 (A)) by gaining on the bound for the number of lattice points in a spherical segment of direction α (compare Propositions 4.5.2 and 4.7.3); this is because we approximate one irrational number instead of two simultaneously (compare Lemmas 4.5.6 and 4.7.2).

Diophantine approximation. The following is the one-dimensional analogue of Proposition 2.1.3.

Proposition 4.7.1 (Dirichlet)**.** *Given $\zeta \in \mathbb{R} \setminus \mathbb{Q}$ and an integer $H \geq 1$, there exist $p, q \in \mathbb{Z}$ so that $1 \leq q \leq H$ and*

$$\left|\zeta - \frac{p}{q}\right| < \frac{1}{qH}.$$

Lemma 4.7.2. *Let $\alpha \in \mathbb{R}^3$ with $\|\alpha\| = 1$ and satisfying $\alpha_2/\alpha_1 \in \mathbb{Q}$ and $\alpha_3/\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$. Write $\alpha_2/\alpha_1 = u/v$ with $u, v \in \mathbb{Z}$ and $v > 0$. Define*

$$\tau = \tau_\alpha := \max\left(|u|, v, \frac{1}{|\alpha_1|}\right) + 1. \tag{4.7.1}$$

Then for all integers $H \geq 1$, there exists $a \in \mathbb{Z}^3$ satisfying

$$\begin{cases} \|a\| < \sqrt{3}\tau_\alpha^2 H & (4.7.2) \\ \left\|\alpha - \dfrac{a}{\|a\|}\right\| < 2\sqrt{3} \cdot \dfrac{\tau_\alpha^2}{\|a\| H}. & (4.7.3) \end{cases}$$

Proof. Take $\zeta = \frac{\alpha_3}{\alpha_1}$ and a large integer H. By Proposition 4.7.1, there exist $p, q \in \mathbb{Z}$ so that $1 \leq q \leq H$ and

$$\left|\frac{\alpha_3}{\alpha_1} - \frac{p}{q}\right| < \frac{1}{qH}.$$

Assume $\alpha_1 > 0$ (in case $\alpha_1 < 0$, take $-\alpha$). Fix $a := (qv, qu, pv)$ and let us show this vector satisfies both (4.7.2) and (4.7.3). We have

$$\left|\frac{p}{q}\right| \leq \left|\frac{\alpha_3}{\alpha_1}\right| + \frac{1}{qH} < \frac{1}{\alpha_1} + 1 \leq \tau \Rightarrow |p| < \tau q$$
$$\Rightarrow \|a\|^2 = q^2v^2 + q^2u^2 + p^2v^2 < \tau^2q^2 + \tau^2q^2 + \tau^4q^2 < 3\tau^4q^2$$

so that
$$\|a\| < \sqrt{3}\tau^2 q \leq \sqrt{3}\tau^2 H \tag{4.7.4}$$
and (4.7.2) is verified. We now turn to proving (4.7.3). We define the vector $d := \frac{\alpha_1}{qv} \cdot a$, hence (as $\alpha_1 > 0$)
$$\frac{d}{\|d\|} = \frac{\frac{\alpha_1}{qv} \cdot a}{\frac{|\alpha_1|}{|qv|} \cdot \|a\|} = \frac{a}{\|a\|}.$$

Apply Lemma 4.5.5 with $w = \alpha$ and $v = d$, recalling $\|\alpha\| = 1$:
$$\left\|\alpha - \frac{a}{\|a\|}\right\| = \left\|\frac{\alpha}{\|\alpha\|} - \frac{d}{\|d\|}\right\| \leq 2\frac{\|\alpha - d\|}{\|\alpha\|} = 2\|\alpha - d\|. \tag{4.7.5}$$
Moreover,
$$\begin{aligned}\|\alpha - d\| &= \left\|\alpha - \frac{\alpha_1}{qv} \cdot a\right\| = \left\|\left(\alpha_1 - \frac{\alpha_1}{qv} \cdot qv, \alpha_2 - \frac{\alpha_1}{qv} \cdot qu, \alpha_3 - \frac{\alpha_1}{qv} \cdot pv\right)\right\| \\ &= |\alpha_1| \cdot \left\|\left(0, \frac{\alpha_2}{\alpha_1} - \frac{u}{v}, \frac{\alpha_3}{\alpha_1} - \frac{p}{q}\right)\right\| = |\alpha_1| \cdot \left\|\left(0, 0, \frac{\alpha_3}{\alpha_1} - \frac{p}{q}\right)\right\| < \frac{1}{qH}. \end{aligned} \tag{4.7.6}$$
By (4.7.4),
$$\frac{1}{q} < \frac{\sqrt{3}\tau^2}{\|a\|}. \tag{4.7.7}$$
Combining (4.7.5), (4.7.6) and (4.7.7),
$$\left\|\alpha - \frac{a}{\|a\|}\right\| \leq 2\|\alpha - d\| < 2 \cdot \frac{1}{qH} < 2\sqrt{3} \cdot \frac{\tau^2}{\|a\|H}$$
and (4.7.3) is verified. □

Recall the notation (4.4.5) for ψ, the maximal number of lattice points in a spherical segment.

Proposition 4.7.3. *Let $S \subset R\mathcal{S}^2$ be a spherical segment of opening angle θ, radius of larger base k, and direction β, with $\frac{\beta_2}{\beta_1} \in \mathbb{Q}$ and $\frac{\beta_3}{\beta_1} \in \mathbb{R} \setminus \mathbb{Q}$. Then the maximal number of lattice points lying on S satisfies*
$$\psi \ll_\beta \kappa(R)(1 + R \cdot \theta^{1/2})$$
for $\theta \to 0$.

Proof. Recall (4.5.17):

$$\psi \ll \kappa(R) \cdot \left[1 + R\left(\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\|\right)\right]. \tag{4.7.8}$$

It then suffices to bound

$$\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\|.$$

We apply Lemma 4.7.2 with $\alpha = \beta$: for all integers $H \geq 1$, there exists $a = (a_1, a_2, a_3)$ so that

$$\|a\|\theta + \|a\| \left\|\beta - \frac{a}{\|a\|}\right\| < \sqrt{3}\tau_\beta^2 H \cdot \theta + 2\sqrt{3} \cdot \frac{\tau_\beta^2}{H} \ll_\beta H \cdot \theta + \frac{1}{H},$$

with τ_β as in (4.7.1). The tradeoff gives us the choice $H = \left\lfloor \frac{1}{\theta^{1/2}} \right\rfloor$, hence

$$\|a\|\theta + \left\|\beta - \frac{a}{\|a\|}\right\| \ll_\beta \theta^{1/2}. \tag{4.7.9}$$

The statement of the present proposition follows on inserting (4.7.9) into (4.7.8). □

Proof of Theorem 1.3.3 (B).

Proof of Theorem 1.3.3 (B). We will follow the proof of Theorem 1.3.3 (A), except the maximal number of lattice points in spherical segments of opening angle θ will be bounded via Proposition 4.7.3 instead of Proposition 4.5.2. Let $\rho = \rho(R)$ be a parameter such that $\rho \to 0$ as $R \to \infty$. We need to bound the two summations on the RHS of (4.6.1). For the former, we use (4.6.2) and (4.6.3); we gain on the estimate (4.6.4) by invoking Proposition 4.7.3 with $\theta = 8\rho + O(\rho^3)$:

$$\sum_\mu \#\{\mu' : \mu' \in S_\mu\} \leq \sum_\mu \psi \ll \mathcal{N} \cdot \kappa(R)(1 + R \cdot \rho^{1/2}). \tag{4.7.10}$$

By substituting (4.6.3) and (4.7.10) into (4.6.2), we get the following bound for the first summation on the RHS of (4.6.1):

$$\begin{aligned}\#\{(\mu, \mu') : |\langle \mu - \mu', \alpha\rangle| \leq \rho \cdot \|\mu - \mu'\|\} &\ll R^\epsilon + \mathcal{N} \cdot \kappa(R)(1 + R \cdot \rho^{1/2}) \\ &\ll R^\epsilon \mathcal{N}(1 + R \cdot \rho^{1/2}). \end{aligned} \tag{4.7.11}$$

For the second summation on the RHS of (4.6.1), we have the bound (4.6.6). Inserting (4.7.11) and (4.6.6) into (4.6.1), and recalling (1.3.5), we deduce

$$\begin{aligned}\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) &\ll \frac{1}{\mathcal{N}^2}R^\epsilon\mathcal{N}\left(\left(1+R\cdot\rho^{1/2}\right)+\frac{\mathcal{N}}{\rho^2R^2}\right)\\ &\ll \frac{1}{\mathcal{N}^2}R^\epsilon\mathcal{N}\left(R\cdot\rho^{1/2}+\frac{1}{\rho^2R}\right).\end{aligned}$$

The optimal choice for the parameter is $\rho=\frac{1}{R^{4/5}}$, thus

$$\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{\mathcal{N}\cdot R^{3/5+\epsilon}}{\mathcal{N}^2} \ll \frac{1}{m^{1/5-\epsilon}}.$$

□

4.8 Conditional result: proof of Theorem 1.3.5

Recall the Definitions 4.4.1 of a spherical cap and 4.4.3 of a spherical segment.

Lemma 4.8.1. *Given $0<c<R$, fix a point $B\in R\mathcal{S}^2$, and let β be a unit vector. Then all points $B'\in R\mathcal{S}^2$ satisfying $|\langle B-B',\beta\rangle|\leq c$ lie either on the same spherical segment, of height $2c$ and direction β, or on the same spherical cap, of height at most $2c$ and direction β, on $R\mathcal{S}^2$.*

Proof. For a real number ξ, define the plane

$$\Pi_\xi : \langle\beta,(x,y,z)\rangle=\xi,$$

orthogonal to β. For $-c\leq c'\leq c$, the condition

$$\langle B-B',\beta\rangle=c' \Leftrightarrow \langle\beta,B'\rangle=\langle\beta,B\rangle-c'$$

means B' lies on the plane $\Pi_{\langle\beta,B\rangle-c'}$. Therefore, all B' satisfying $|\langle B-B',\beta\rangle|\leq c$ belong to a region $\mathcal{R}$ of $\mathbb{R}^3$ delimited by two parallel planes, namely $\Pi_{\langle\beta,B\rangle-c}$ and $\Pi_{\langle\beta,B\rangle+c}$. The distance between these two planes is $2c$. Denote

$$\mathcal{R}'=\mathcal{R}\cap R\mathcal{S}^2.$$

In case $|\langle\beta, B\rangle| < R-c$, both $\Pi_{\langle\beta,B\rangle-c}$ and $\Pi_{\langle\beta,B\rangle+c}$ intersect $R\mathcal{S}^2$ in a circle. By Definition 4.4.3, $\mathcal{R}'$ is then a spherical segment, of height $2c$ and direction β. In case $R-c \leq |\langle\beta, B\rangle| \leq R$, one of the intersections $\Pi_{\langle\beta,B\rangle-c} \cap R\mathcal{S}^2$ and $\Pi_{\langle\beta,B\rangle+c} \cap R\mathcal{S}^2$ is either empty or a single point. By Definition 4.4.1, $\mathcal{R}'$ is then a spherical cap, of height at most $2c$ and direction β. □

Proof of Theorem 1.3.5. Apply Proposition 4.3.2, yielding (4.3.1). Let $0 < \rho < R$ be a parameter and split the summation on the RHS of (4.3.1), applying (4.3.2):

$$\operatorname{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{\mathcal{N}^2} \cdot \left(\sum_{|\langle\mu-\mu',\alpha\rangle|\leq\rho} 1 + \sum_{|\langle\mu-\mu',\alpha\rangle|\geq\rho} \frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right). \tag{4.8.1}$$

For the second summation on the RHS of (4.8.1), we write

$$\sum_{|\langle\mu-\mu',\alpha\rangle|\geq\rho} \frac{1}{\langle\mu-\mu',\alpha\rangle^2} \leq \frac{1}{\rho^2} \sum_{|\langle\mu-\mu',\alpha\rangle|\geq\rho} 1 \leq \frac{\mathcal{N}^2}{\rho^2}. \tag{4.8.2}$$

For the remaining summation in (4.8.1), we show that there are few pairs (μ, μ') satisfying $|\langle\mu-\mu', \alpha\rangle| \leq \rho$. Fix a lattice point μ and apply Lemma 4.8.1 with $\beta = \alpha$ and $c = \rho$: then μ' verifies $|\langle\mu-\mu', \alpha\rangle| \leq \rho$ if and only if it lies on a spherical segment S_μ of height 2ρ and direction α, or on a spherical cap T_μ of height at most 2ρ and direction α. That is to say,

$$\begin{aligned} \#\{(\mu,\mu') : |\langle\mu-\mu',\alpha\rangle| \leq \rho\} &\leq \sum_\mu \#\{\mu' : \mu' \in T_\mu\} + \sum_\mu \#\{\mu' : \mu' \in S_\mu\} \\ &\leq 2 \cdot \#\{(\mu,\mu') : \mu,\mu' \in T\} + \sum_\mu \#\{\mu' : \mu' \in S_\mu\}, \end{aligned} \tag{4.8.3}$$

where T is the spherical cap of height 2ρ and direction α. By Conjecture 1.3.4, the maximal number of lattice points in a cap of radius s of the sphere $R\mathcal{S}^2$ satisfies $\chi(R,s) \ll R^\epsilon(1+\frac{s^2}{R})$. Therefore, recalling (4.4.1),

$$\#\{\mu : \mu \in T\} \ll R^\epsilon \left(1 + \frac{s^2}{R}\right) \ll R^\epsilon(1+\rho),$$

and it follows that

$$\#\{(\mu,\mu') : \mu,\mu' \in T\} \ll R^{\epsilon}(1+\rho^2). \tag{4.8.4}$$

To bound the number of lattice points in the spherical segment S_μ, we may apply Corollary 4.4.8 with $h = 2\rho$. We then get

$$\sum_{\mu} \#\{\mu' : \mu' \in S_\mu\} \ll \mathcal{N} \cdot R^{\epsilon} \cdot (R^{1/2} + \rho). \tag{4.8.5}$$

Inserting the estimates (4.8.4) and (4.8.5) into (4.8.3), and then the inequalities (4.8.3) and (4.8.2) into (4.8.1) gives us

$$\mathrm{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{1}{\mathcal{N}^2} \cdot \left(\frac{\mathcal{N}^2}{\rho^2} + R^{\epsilon}\left(1+\rho^2+\mathcal{N}R^{1/2}+\mathcal{N}\rho\right)\right).$$

Taking any ρ in the range $R^{1/4} \leq \rho \leq R^{1/2}$ and recalling (1.3.5), we obtain

$$\mathrm{Var}\left(\frac{\mathcal{Z}}{\sqrt{m}}\right) \ll \frac{\mathcal{N} \cdot R^{1/2+\epsilon}}{\mathcal{N}^2} \ll \frac{1}{m^{1/4-\epsilon}}.$$

$\square$

Chapter 5

Nodal area of 3D arithmetic random waves

The present chapter incorporates the publication [4], in collaboration with Jacques Benatar. We will prove Theorems 1.4.1, 1.4.3 and 1.4.4, and Corollary 1.4.5.

5.1 Outline

Recall the notation for the lattice point set $\mathcal{E} = \mathcal{E}^{(3)}$ and its cardinality $\mathcal{N}$. Our setting is the ensemble of arithmetic random waves on the three-dimensional torus (1.3.3)

$$F(x) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{(\mu^{(1)},\mu^{(2)},\mu^{(3)})\in\mathcal{E}} a_\mu e^{2\pi i\langle\mu,x\rangle},$$

and we are interested in the distribution of the nodal area (1.4.7)

$$\mathcal{A} := \text{Vol}(\{x \in \mathbb{T}^3 : F(x) = 0\}).$$

In this chapter, we prove Theorems 1.4.3 and 1.4.4, and Proposition 1.4.2. We note that Theorem 1.4.1 follows immediately.

Proof of Theorem 1.4.1. Insert the bounds of Theorems 1.4.3 and 1.4.4 into Proposition 1.4.2. □

The proof of Proposition 1.4.2 begins in section 5.4 and is concluded in section 5.5, after the necessary preparatory results have been stated. The proof follows the method employed in [47] for the 2-dimensional case. In section 5.4.1, we apply Kac-Rice formulas to study the nodal area variance, since the arithmetic random wave (1.3.3) is a Gaussian random field (see section 2.4.4). To this purpose, it is necessary to understand the two-point correlation function $\tilde{K}_2$ of F (recall (2.4.9)). In section 5.4.2, we express K_2, a scaled version of $\tilde{K}_2$, in terms of the conditional Gaussian expectation of the 6×6 vector $(\nabla F(0), \nabla F(x))$ conditioned on $F(0) = 0, F(x) = 0$. The resulting (scaled) covariance matrix, Ω, depends on the covariance function (2.4.2) of F,

$$r_F(x,y) := \mathbb{E}[F(x)\cdot F(y)] = \frac{1}{\mathcal{N}}\sum_{\mu\in\mathcal{E}} e^{2\pi i\langle \mu,(x-y)\rangle}, \tag{5.1.1}$$

and its (first and second order) derivatives.

Next, in section 5.5, we define a small set $S\subset\mathbb{T}^3$ (the *singular set*, cf. Definition 5.5.3), where it is possible to bound the contribution of K_2 to the variance. We then establish asymptotics for K_2 valid outside the set S: this computation involves the Taylor expansion of K_2 as a 6-variate function of Ω around the identity matrix I_6; in fact, we will show that, on $\mathbb{T}^3\setminus S$, Ω is a small perturbation of I_6. The Taylor expansion is carried out in appendix C, using Berry's elegant method [5]. In section 5.6 we perform the technical computations needed to evaluate the leading constant of the nodal area variance; the necessary background on spherical lattice points is covered in section 5.2.

Let us highlight similarities and differences with the 2-dimensional setting [47]. Both the leading term and error term in Proposition 1.4.2 are of arithmetic nature, as in [47]: the leading term depends on the angular distribution of lattice points on spheres, while the error term depends on the lattice point correlations of Definition 2.2.14. However, there are marked differences between the 2- and 3-dimensional settings; first, as noted above, the nodal area variance obeys an asymptotic law, whereas the nodal *length* variance depends on arithmetic properties of the energy.

Second, for the admissibility of the error term, we require a bound for the number of non-degenerate spectral correlations of length 4, $|\mathcal{X}_m^{(3)}(4)|$ (recall Definition 2.2.14) whereas, in the 2-dimensional setting, one has (2.2.18)

$$|\mathcal{X}_m^{(2)}(4)| = 0 \qquad \text{for all } m \in S^{(2)},$$

by "Zygmund's trick". The bound for the length four correlations of Theorem 1.4.3 will be established in section 5.3.1.

One must also bound the total number of length six correlations $|\mathcal{C}_m(6)|$. The proof of Theorem 1.4.4 will be established in section 5.3.2 via a theorem due to Fox-Pach-Sheffer-Suk-Zahl [33]. Their result allows one to bound the number of incidences between points and spheres in $\mathbb{R}^3$, thereby playing the role of the Szemerédi-Trotter Theorem employed in dimension 2 [6, 47] (also see section 2.2.5).

5.2 Lattice points on spheres and spectral correlations

Recall the notation for the lattice point set $\mathcal{E}_m$ and its cardinality $\mathcal{N}_m$. As mentioned in sections 1.3 and 2.2.3, $\mathcal{E}_m$ is non-empty if and only if m is not of the form $4^l(8k+7)$. We work with the assumption $m \not\equiv 0, 4, 7 \pmod 8$, which is equivalent to the existence of lattice points $(\mu^{(1)}, \mu^{(2)}, \mu^{(3)}) \in \mathcal{E}_m$ with $\mu^{(1)}, \mu^{(2)}, \mu^{(3)}$ coprime. In this case, the quantities $\mathcal{N}_m$ and m are related by the estimates (1.3.5)

$$m^{1/2-o(1)} \ll \mathcal{N}_m \ll m^{1/2+o(1)}.$$

We also recall Jarnik's upper bound (1.3.9)

$$\kappa(m) \ll m^{o(1)} \tag{5.2.1}$$

for the number of lattice points lying on the intersection with a plane.

Recall the notation for the k-th moment of the normalised inner product of two lattice points ((2.2.11) with $d = 3$)

$$B_k = B_k^{(3)}(m) := \frac{1}{m^k \mathcal{N}^2} \sum_{\mu_1,\mu_2 \in \mathcal{E}} \langle \mu_1, \mu_2 \rangle^k. \tag{5.2.2}$$

This arithmetic quantity arises naturally in the computation of the leading term of the variance (see section 5.6 to follow).

Lemma 5.2.1. *We have:*

$$B_k = \begin{cases} 0 & \textit{for odd } k; \\ 1/3 & \textit{for } k = 2; \\ \frac{1}{k+1} + O\left(\frac{1}{m^{1/28-o(1)}}\right) & \textit{for even } k \geq 4, \ \textit{as } m \to \infty, \ m \not\equiv 0, 4, 7 \pmod 8. \end{cases}$$

In particular,

$$B_4 = \frac{1}{5} + O\left(\frac{1}{m^{1/28-o(1)}}\right). \tag{5.2.3}$$

Proof. This is the special case $d = 3$ of Lemma 2.2.13. □

With the notation introduced in section 1.1, we shall write the coordinates of a lattice point as

$$\mu = (\mu^{(1)}, \mu^{(2)}, \mu^{(3)}) \in \mathcal{E},$$

whereas the expression

$$(\mu_1, \mu_2, \ldots, \mu_\ell) \in \mathcal{E}^\ell$$

will indicate an ℓ-tuple of lattice points. Recall Definition 2.2.14 of the set of ℓ-spectral correlations $\mathcal{C}_m^{(d)}(\ell)$. Let us analyse in detail the set $\mathcal{C}(4) = \mathcal{C}_m^{(3)}(4)$, as several summations range over this set in what follows. Let $d = 3$ and $\ell = 4$

in Definitions 2.2.14. Then $\mathcal{D}(4) = \mathcal{D}'(4)$ is the set of quadruples $(\mu_1, \mu_2, \mu_3, \mu_4)$ that cancel out in pairs,

$$\mu_1 = -\mu_2 \text{ and } \mu_3 = -\mu_4,$$

and permutations of the indices (i.e., each degenerate correlation is necessarily symmetric when $\ell = 4$). The diagonal correlations $\mathcal{D}'' \subset \mathcal{D}$ satisfy

$$\mu_1 = \mu_2 = -\mu_3 = -\mu_4$$

for some permutation of the indices. With $\mathcal{X}(4)$ denoting as usual the set of non-degenerate correlations, a summation over $\mathcal{C}(4)$ may thus be treated by separating it as follows:

$$\sum_{\mathcal{C}(4)} = \sum_{\substack{\mu_1=-\mu_2\\ \mu_3=-\mu_4}} + \sum_{\substack{\mu_1=-\mu_3\\ \mu_2=-\mu_4}} + \sum_{\substack{\mu_1=-\mu_4\\ \mu_2=-\mu_3}} + O\left(\sum_{\mathcal{D}''} + \sum_{\mathcal{X}(4)}\right). \tag{5.2.4}$$

Pairs of lattice points with fixed inner product. The proof of Theorem 1.4.3 will rely on a classical estimate regarding the size of the set

$$I_m(r) := \left\{(\mu_1, \mu_2) \in \mathcal{E}_m^2 : \langle \mu_1, \mu_2 \rangle = r\right\} = \left\{(\mu_1, \mu_2) \in \mathcal{E}_m^2 : \|\mu_1 + \mu_2\|^2 = 2(m + r)\right\}.$$

In fact, there is an exact formula for $|I_m(r)|$ (see [56, section 7]) from which one can deduce the following bound.

Theorem 5.2.2 (Pall [56])**.** *For $|r| < m$ one has that*

$$|I_m(r)| \ll \gcd(r, m)^{1/2} m^{o(1)}.$$

Before proceeding to the next lemma we introduce some notation. Given $a \in \mathbb{N}$ write $a_m := \gcd(a, m)$, yielding the corresponding decomposition $a = a_m a'$. For any interval $J \subset (0, 4m)$ we may now introduce the collection

$$\mathcal{J}_m(J, a) = \left\{\tau \in \mathcal{E}_m + \mathcal{E}_m : \|\tau\|^2 \in J,\ \|\tau\|^2 \equiv 0 \pmod{a}\right\}.$$

Lemma 5.2.3. *(i) For any $\mathcal{B} \subset \mathcal{E}_m + \mathcal{E}_m$ satisfying the bound $|\{\|\tau\|^2 : \tau \in \mathcal{B}\}| \leq T$ one has that $|\mathcal{B}| \ll \mathcal{N}^{1+o(1)} T^{1/2}$.*

(ii) Given any natural number $a = a_m a'$ and any interval $J \subset (0, 4m)$ we have the estimate

$$|\mathcal{J}_m(J,a)| \leq \mathcal{N}^{o(1)} \left(\frac{|J|}{(a_m)^{1/2} a'} + \frac{\mathcal{N}}{(a')^{1/2}} \right).$$

Proof. (i) Given any $d|m$ the number of $\tau \in \mathcal{B}$ for which

$$\gcd\left(\frac{\|\tau\|^2 - 2m}{2}, m \right) = d \tag{5.2.5}$$

is at most

$$\sum_{|l|<m/d}' \left| \left\{ \tau \in \mathcal{B} : \frac{\|\tau\|^2 - 2m}{2} = ld \right\} \right| \leq \max_{\substack{\mathcal{L} \subset (-m/d, m/d) \cap \mathbb{Z} \\ |\mathcal{L}| \leq T}} \sum_{l \in \mathcal{L}}' |I_m(ld)|, \tag{5.2.6}$$

where the superscript $'$ indicates a summation over integers l for which $\gcd(ld, m) = d$.

We first consider divisors in the range $d \geq m/T$. Applying Theorem 5.2.2 we gather that the RHS of (5.2.6) is no greater than

$$\sum_{l \leq m/d} d^{1/2} m^{o(1)} \ll \frac{m^{1+o(1)}}{d^{1/2}} \ll \mathcal{N}^{1+o(1)} T^{1/2}.$$

On the other hand, when $d < m/T$ the RHS of (5.2.6) is $O(d^{1/2} m^{\epsilon} T) = O(\mathcal{N}^{1+o(1)} T^{1/2})$. Adding the contribution of each divisor d we get the desired estimate.

(ii) We repeat the argument given in (i) and consider for each divisor $d|m$ the vectors $\tau \in \mathcal{J}_m(J,a)$ for which (5.2.5) holds. In particular we must have that $a_m|d$ and it is not hard to show that $\|\tau\|^2 \equiv 0 \pmod{da'}$ which implies the bound $d \leq 4m/a'$. Setting $J' := J/2 - m$, the inequality (5.2.6) becomes

$$\sum_{|l|<m/d}' \left|\left\{\tau \in \mathcal{J}_m(J,a) : \frac{\|\tau\|^2 - 2m}{2} = ld\right\}\right| \leq \sum_{\substack{l \in J'/d \\ l \equiv -m/d \pmod{a'}}}' |I_m(ld)|$$
$$\ll \mathcal{N}^{o(1)} \cdot d^{1/2}\left(\frac{|J'|}{da'} + 1\right) \ll \mathcal{N}^{o(1)} \cdot \left(\frac{|J'|}{a_m^{1/2} a'} + \left(\frac{m}{a'}\right)^{1/2}\right).$$

Noting that $|J'| < |J|$ we add the contribution of each d to conclude the lemma.

□

5.3 Spectral correlations

Length four correlations: proof of Theorem 1.4.3

In this subsection, we prove Theorem 1.4.3. For fixed $\mu_1, \mu_2 \in \mathcal{E}_m$ (with $\mu_1 \neq -\mu_2$), write $\tau = (t_1, t_2, t_3) := -(\mu_1 + \mu_2)$. Clearly any pair of points $\mu_3, \mu_4 \in \mathcal{E}_m$ satisfying

$$\mu_3 + \mu_4 = \tau \tag{5.3.1}$$

must both lie on the intersection of the two spheres of radius $\sqrt{m}$ centred at the origin and at τ. This resulting intersection is a circle of radius

$$\rho = \left(m - \frac{1}{4}\|\tau\|^2\right)^{1/2},$$

centred at $\tau/2$, and confined to the plane

$$\left\{x \in \mathbb{R}^3 : \langle 2\tau, x\rangle = \|\tau\|^2\right\}.$$

As a consequence we may count the number of pairs (μ_3, μ_4) satisfying (5.3.1) by estimating the size of the set $\tilde{\mathcal{X}}(\tau)$ consisting of those integer lattice points which lie in the plane

$$P : \langle \tau, x \rangle = 0, \qquad x \in \mathbb{R}^3 \tag{5.3.2}$$

and have norm

$$2\rho = (4m - \|\tau\|^2)^{1/2}.$$

A bound for $\mathcal{X}_m(4)$ is then given by

$$|\mathcal{X}_m(4)| \ll \sum_{\tau \in \mathcal{E}_m + \mathcal{E}_m} \sum_{\substack{\mu_1, \mu_2 \in \mathcal{E}_m \\ \mu_1 + \mu_2 = \tau}} \left(|\tilde{\mathcal{X}}(\tau)| - 2 \right), \tag{5.3.3}$$

where the summation takes into account only those pairs (μ_1, μ_2) for which $\tilde{\mathcal{X}}(\tau)$ contains at least two non-antipodal points. In the remainder of this subsection we will seek to bound the size of the set

$$\mathcal{T} := \{\tau \in \mathcal{E}_m + \mathcal{E}_m : |\tilde{\mathcal{X}}(\tau)| > 2\}.$$

Proposition 5.3.1. *With the above notation we have the estimate* $|\mathcal{T}| \ll \mathcal{N}^{7/4+o(1)}$.

Let us first prove Theorem 1.4.3 assuming Proposition 5.3.1.

Proof of Theorem 1.4.3. By (5.2.1) one has the general upper bound $|\tilde{\mathcal{X}}(\tau)| \ll m^{o(1)}$ whenever $\tau \neq 0$. Inserting both this estimate and the bound of Proposition 5.3.1 into (5.3.3) we obtain our result. □

The proof of Proposition 5.3.1. In order to understand $\tilde{\mathcal{X}}(\tau)$, we begin with a simple description of the lattice $P \cap \mathbb{Z}^3$, where P is the plane (5.3.2). Some general background on lattices was given in section 2.1.4. Recalling the notation $\tau = (t_1, t_2, t_3)$ let us first set $\gcd(t_1, t_2, t_3) = s$ and write $\tau' = (t'_1, t'_2, t'_3) := \frac{1}{s}\tau$. Since τ' is primitive, $P \cap \mathbb{Z}^3$ has determinant $\|\tau'\|$ (cf. the corollary [17, page

25]) and hence there exist vectors $A, B \in \mathbb{Z}^3$ with $A \times B = \tau'$. A generic lattice point in P may be expressed as $kA + lB$ with $k, l \in \mathbb{Z}$.

Let us suppose $\tau \in \mathcal{T}$ and write $n := 4m - \|\tau\|^2$. As $\tau \in \mathcal{T}$, there must be two non-antipodal vectors $C = k_1 A + l_1 B$ and $D = k_2 A + l_2 B$ for which

$$\|C\|^2 = \|D\|^2 = n.$$

Setting $r := k_1 l_2 - k_2 l_1$ we observe that $C \times D = r(A \times B) = \frac{r}{s}\tau$ and record the inequality

$$\|\tau\|^2 \leq \frac{16 s^2 m^2}{r^2}. \tag{5.3.4}$$

Moreover, noting that $\|C \times D\|^2 = n^2 - \langle C, D\rangle^2$ we obtain the identity

$$\frac{s^2}{r^2}\left(n^2 - \langle C, D\rangle^2\right) + n = 4m.$$

Multiplying both sides of the equation by $4r^2s^2$ one gets the rearranged expression

$$(2s^2 n + r^2)^2 - \left(2s^2\langle C, D\rangle\right)^2 = 16mr^2s^2 + r^4$$

and hence

$$\left(2s^2 n + r^2 - 2s^2\langle C, D\rangle\right)\left(2s^2 n + r^2 + 2s^2\langle C, D\rangle\right) = 16mr^2s^2 + r^4. \tag{5.3.5}$$

Assuming the equation (5.3.5) has solutions, there must exist a positive $d | 16mr^2s^2 + r^4$ (given by either factor on the LHS of (5.3.5)) so that

$$4s^2 n + 2r^2 = d + \frac{1}{d}\left(16mr^2s^2 + r^4\right). \tag{5.3.6}$$

To count the number of vectors $\tau \in \mathcal{T}$ we will consider equation (5.3.6) in each dyadic interval $r \in [R, 2R], s \in [S, 2S]$. Here R and S are dyadic powers in the ranges $1 \leq R \leq 2m$ and $1 \leq S \leq m^{1/2}$.

Lemma 5.3.2. *With R, S as above let $\mathcal{T}(R, S)$ denote the set of $\tau \in \mathcal{T}$ which satisfy equation* (5.3.6) *for some pair of integers $(r, s) \in [R, 2R] \times [S, 2S]$. Then*

$$|\mathcal{T}(R, S)| \ll \mathcal{N}^{o(1)} \min\left(\frac{m}{S} + \mathcal{N}, \frac{Sm^2}{R^2} + \mathcal{N}, \mathcal{N} R^{1/2} S^{1/2}\right). \tag{5.3.7}$$

Proof. Given $\tau \in \mathcal{T}(R,S)$ with its associated quadruple (n,r,s,d) we recall that

$$\|\tau\|^2 \equiv 0 \pmod{s^2}.$$

Setting $s_m := \gcd(s,m)$ we may write $s = s_m s'$ and put $\nu := \gcd(s^2, m)$. Clearly $s_m|\nu$ and $\nu|(s_m)^2$ so we are led to a decomposition of the form

$$\nu = s_m\sigma_1, \qquad s_m = \sigma_1\sigma_2$$

which yields $s^2 = \nu(\sigma_2(s')^2)$. It follows from Lemma 5.2.3 part (ii) (with $J = (0,4m)$ and $a = s^2$) and the inequality $(s_m\sigma_1)^{1/2}\sigma_2 \geq (s_m\sigma_1\sigma_2)^{1/2} = s_m$ that

$$\begin{aligned} |\mathcal{T}(R,S)| &\ll \sum_{\substack{s_m|m \\ s_m\leq 2S}} \sum_{s'\asymp S/s_m} \sum_{\sigma_1\sigma_2=s_m} \mathcal{N}^{o(1)}\left(\frac{m}{(s_m\sigma_1)^{1/2}\sigma_2(s')^2} + \frac{\mathcal{N}}{(\sigma_2)^{1/2}s'}\right) \\ &\ll \sum_{\substack{s_m|m \\ s_m\leq 2S}} \sum_{s'\asymp S/s_m} \mathcal{N}^{o(1)}\left(\frac{m}{s_m(s')^2} + \frac{\mathcal{N}}{s'}\right) \\ &\ll \mathcal{N}^{o(1)}\left(\frac{m}{S} + \mathcal{N}\right), \end{aligned} \tag{5.3.8}$$

yielding the first inequality in (5.3.7). In light of (5.3.4) we may reuse the estimates given in (5.3.8), this time applying Lemma 5.2.3 part (ii) with the interval $J = (0, 16s^2m^2/R^2)$. The bound $|\mathcal{T}(R,S)| \ll \mathcal{N}^{o(1)}(Sm/R^2 + \mathcal{N})$ follows readily.

A brief inspection of (5.3.6) reveals that for each choice of $(r,s) \in [R,2R] \times [S,2S]$ and each choice of divisor $d|16mr^2s^2 + r^4$, the value of n is uniquely determined. In this manner we get $O(\mathcal{N}^{o(1)}RS)$ possible values of n and hence the final estimate in (5.3.7) follows from an application of Lemma 5.2.3 part (i). $\square$

To conclude the proof of Proposition 5.3.1, we note that

$$|\mathcal{T}| \leq \sum_{R,S} |\mathcal{T}(R,S)|$$

and apply the estimates of Lemma 5.3.2 to get

$$|\mathcal{T}| \ll \sum_{\substack{R \leq 2m, S \leq m^{1/2} \\ \text{dyadic}}} \mathcal{N}^{o(1)} \min\left(\mathcal{N} R^{1/2} S^{1/2}, \frac{Sm^2}{R^2}, \frac{m}{S}\right) + \mathcal{N}^{1+o(1)}.$$

For fixed S, the largest possible value of $\min(\mathcal{N} R^{1/2} S^{1/2}, Sm^2/R^2)$ occurs when $R \asymp S^{1/5} m^{4/5} / \mathcal{N}^{2/5}$. Recalling the relation between m and $\mathcal{N}$ (1.3.5),

$$\min(\mathcal{N} R^{1/2} S^{1/2}, Sm^2/R^2) \ll \mathcal{N}^{8/5+o(1)} S^{3/5}.$$

It follows that

$$|\mathcal{T}| \ll \sum_{S \leq m^{1/2}} \mathcal{N}^{o(1)} \min\left(\mathcal{N}^{8/5} S^{3/5}, \frac{m}{S}\right) + \mathcal{N}^{1+o(1)} \ll \mathcal{N}^{7/4+o(1)}.$$

Length six correlations: proof of Theorem 1.4.4

In this subsection, we prove Theorem 1.4.4. The key ingredient is the incidence bound [33, Theorem 6.4], which we state below in a simplified form. Given a collection of points $\mathcal{P}$ and a collection of varieties $\mathcal{V}$, we define

$$I(\mathcal{P}, \mathcal{V}) := \#\{(p, V) \in \mathcal{P} \times \mathcal{V} : p \in V\}$$

to be the number of **incidences** between $\mathcal{P}$ and $\mathcal{V}$. We will use the standard notation $K_{s,t}$ for complete bipartite graphs. Given graphs G and H, we say G is H-free if it does not contain an induced subgraph isomorphic to H.

Theorem 5.3.3 ([33]). *Let $\mathcal{P} \subset \mathbb{R}^3$ be a set of k points and $\mathcal{V}$ a collection of n varieties of bounded degree in $\mathbb{R}^3$. Assuming the incidence graph of $\mathcal{P} \times \mathcal{V}$ is $K_{s,t}$-free there exists, for each $\epsilon > 0$, a positive constant $c = c(\epsilon)$ so that*

$$I(\mathcal{P}, \mathcal{V}) \leq stc\left(k^{\frac{2s}{3s-1}+\epsilon} \cdot n^{\frac{3(s-1)}{3s-1}} + (k+n)\right). \tag{5.3.9}$$

The inequality (5.3.9) gives a polynomial dependence in t which will be crucial to the argument in this subsection. Although not explicitly stated in the above form one can follow the proofs given in [33, Theorems 4.3 and 6.4] and keep track of all the constants involved.

To prove Theorem 1.4.4, we will apply Theorem 5.3.3 with the set of points

$$\mathcal{P} = \mathcal{E} + \mathcal{E}$$

and varieties (spheres)

$$\mathcal{S} = \left\{ \{\|x - A\|^2 = m\} : A \in \mathcal{E} + \mathcal{E} + \mathcal{E} \right\}.$$

For fixed $\epsilon > 0$ and m sufficiently large we set $s = 2$ and $t = \mathcal{N}^\epsilon$ and observe that, by (5.2.1), the incidence graph of $\mathcal{P} \times \mathcal{S}$ is $K_{s,t}$-free. The remainder of the argument is carried out as in [6, section 2] with Theorem 5.3.3 replacing the Szemerédi-Trotter Theorem. For any dyadic power $D \geq 1$ denote by $\mathcal{S}(D)$ the collection of spheres $S = \{\|x - A\|^2 = m\} \in \mathcal{S}$ for which $|S \cap \mathcal{P}| \asymp D$. Recalling (5.2.1) we gather that

$$|\mathcal{C}_m(6)| \ll_\epsilon \mathcal{N}^\epsilon \sum_{\substack{D \leq \mathcal{N} \\ \text{dyadic}}} D^2 |\mathcal{S}(D)|. \tag{5.3.10}$$

Lemma 5.3.4. *For $D \leq \mathcal{N}$ we have the estimates*

$$(i)\ D|\mathcal{S}(D)| \ll \mathcal{N}^3, \qquad (ii)\ D^{5/2}|\mathcal{S}(D)| \ll \mathcal{N}^4.$$

Proof. (i) For each $\tau \in \mathcal{P} = \mathcal{E} + \mathcal{E}$ denote by $\mathcal{S}_\tau(D)$ the collection of spheres in $\mathcal{S}(D)$ which are incident to τ. Then we have the trivial bound

$$D|\mathcal{S}(D)| \leq I(\mathcal{P}, \mathcal{S}(D)) \leq \sum_{\tau \in \mathcal{P}} |\mathcal{S}_\tau(D)| \leq \mathcal{N}^3.$$

(ii) We first note the inequality $|\mathcal{S}(D)| \leq |\mathcal{S}(D)|^{3/5}|\mathcal{P}|^{4/5}$ which follows easily from the rearranged statement $|\mathcal{S}(D)| \leq \mathcal{N}^4$. Applying Theorem 5.3.3 we get the bound

$$\begin{aligned} D|\mathcal{S}(D)| &\ll I(\mathcal{P}, \mathcal{S}(D)) \ll_\epsilon |\mathcal{S}(D)|^{3/5}|\mathcal{P}|^{4/5+\epsilon} + |\mathcal{S}(D)| + |\mathcal{P}| \\ &\leq |\mathcal{S}(D)|^{3/5}|\mathcal{P}|^{4/5+\epsilon} + |\mathcal{P}|. \end{aligned} \tag{5.3.11}$$

When the first term on the RHS of (5.3.11) dominates one finds that $D|\mathcal{S}(D)| \ll |\mathcal{S}(D)|^{3/5}|\mathcal{N}|^{8/5}$ which gives $D^{5/2}|\mathcal{S}(D)| \ll \mathcal{N}^4$. When the second term on the RHS dominates we get $D|\mathcal{S}(D)| \ll \mathcal{N}^2$ so that

$$D^{5/2}|\mathcal{S}(D)| \leq D|\mathcal{S}(D)|\mathcal{N}^{3/2} \ll \mathcal{N}^{7/2}.$$

$\square$

Combining the estimates of the lemma with (5.3.10) we get

$$|\mathcal{C}_m(6)| \ll_\epsilon \mathcal{N}^\epsilon \sum_{D \leq \mathcal{N}} D \cdot \min\left(\mathcal{N}^3, \frac{\mathcal{N}^4}{D^{3/2}}\right) \ll_\epsilon \mathcal{N}^{11/3+\epsilon},$$

which completes the proof of Theorem 1.4.4.

Long correlations: proof of Corollary 1.4.5

In this section we will prove Corollary 1.4.5 via an analytic argument. In what follows, we will use the shorthand $e(z) := e^{2\pi i z}$. We sometimes write $e\langle \cdot, \cdot \rangle$ in place of $e(\langle \cdot, \cdot \rangle)$ to simplify the notation. We introduce the function

$$f(\alpha) := \sum_{\mu \in \mathcal{E}_m} e(\langle \mu, \alpha \rangle)$$

and observe that, by orthogonality,

$$|\mathcal{C}_m(\ell)| = \int_{[0,1]^3} f(\alpha)^\ell d\alpha. \tag{5.3.12}$$

An upper bound for $|\mathcal{C}_m(\ell)|$

Let $\ell \geq 6$ and observe that one has the trivial bound $|f(\alpha)| \leq \mathcal{N}$. By Theorem 1.4.4 and (5.3.12) it follows that

$$|\mathcal{C}_m(\ell)| \leq \mathcal{N}^{\ell-6} \int |f(\alpha)|^6 d\alpha \ll_\epsilon \mathcal{N}^{\ell-7/3+\epsilon}.$$

To conclude the discussion of the upper bounds we record the straightforward estimate

$$\begin{aligned}|\mathcal{C}_m(5)| &\leq \int_{[0,1]^3} |f(\alpha)|^5 d\alpha \leq \left(\int_{[0,1]^3} |f(\alpha)|^4 d\alpha\right)^{1/2} \left(\int_{[0,1]^3} |f(\alpha)|^6 d\alpha\right)^{1/2} \\ &\ll_\epsilon \mathcal{N}^{17/6+\epsilon}\end{aligned}$$

and note that $|\mathcal{C}_m(2)| = \mathcal{N}$ while $|\mathcal{C}_m(3)| \ll \mathcal{N}^{1+o(1)}$ (as a consequence of (5.2.1)).

A lower bound for $|\mathcal{X}_m(\ell)|$

Let $\ell \geq 8$ be even and recall the notation $\mathcal{D}(\ell)$ and $\mathcal{D}'(\ell)$ for the set of degenerate and symmetric tuples respectively. Observe that the degenerate tuples in $\mathcal{C}_m(\ell)$ number at most

$$\begin{aligned}|\mathcal{D}(\ell)| = |\mathcal{D}'(\ell)| + \sum_{\substack{2\leq j_1\leq \ldots \leq j_k \leq \ell-2 \\ j_1+\ldots+j_k=\ell \\ 3\leq j_k}} \prod_{i=1}^{k} |\mathcal{C}_m(j_i)| &\ll \mathcal{N}^{\ell/2} + \mathcal{N}^{(\sum_{i\leq k} j_i)-1-7/3+o(1)} \\ &\ll \mathcal{N}^{\ell-10/3+o(1)}\end{aligned}$$

with the largest contribution coming from the multi-index $j_1 = 2, j_2 = \ell - 2$. As a result it will suffice to prove the asserted lower bound in (1.4.9) for $|\mathcal{C}_m(\ell)|$.

Consider the set

$$A := \left\{\alpha \in [0,1]^3 : |f(\alpha)| \geq \mathcal{N}/2\right\}.$$

Since $f(0) = \mathcal{N}$ and f has partial derivatives of size at most $m^{1/2}\mathcal{N} \ll_\epsilon \mathcal{N}^{2+\epsilon}$, we gather that

$$|f(\alpha) - \mathcal{N}| = |f(\alpha) - f(0)| \leq \|\nabla f\| \cdot \|\alpha\| \leq \mathcal{N}^{2+\epsilon}\|\alpha\|.$$

It follows that $|f(\alpha)| \geq \mathcal{N}/2$ whenever $\|\alpha\| \ll \mathcal{N}^{-1-\epsilon}$ and hence the Lebesgue measure of A is bounded from below by $\lambda(A) \gg_\epsilon \mathcal{N}^{-3-\epsilon}$. Inserting this information into (5.3.12) we find the desired estimate

$$\mathcal{C}_m(\ell) \geq \int_A f(\alpha)^\ell d\alpha \gg_\epsilon \mathcal{N}^{\ell-3-\epsilon}.$$

5.4 Nodal area variance: the setup

Application of Kac-Rice formulas

As the arithmetic random wave F (1.3.3) is a Gaussian field, one may employ Kac-Rice formulas to compute moments of the nodal area. With the notation of section 2.4.1, we write

$$\phi_{F(x)}$$

for the density of the Gaussian variable $F(x)$, and $K_1 : \mathbb{T}^3 \to \mathbb{R}$,

$$K_1 = \phi_{F(y)}(0) \cdot \mathbb{E}[\|\nabla F(y)\| \mid F(y) = 0],$$

for the zero density function (2.4.13) of F, which is independent of y as F is stationary. We wish to apply Theorem 2.4.9 with $B = \mathbb{T}^3$, $Z = F$, $u = 0$ and $t = x$. Let us check the hypotheses: the random field F is of course Gaussian, with smooth paths. Moreover, (iii) must hold as $\mathrm{Var}(F) = r(x) = r(0) = 1$ for all x, while the condition (iv) is satisfied thanks to the following lemma.

Lemma 5.4.1 ([54, Lemma 2.3], [60, Lemma 2.2])**.** *The set of singular eigenfunctions is of measure* 0*.*

We obtain the Kac-Rice formula for the expected nodal area

$$\mathbb{E}[\mathcal{A}] = \int_{\mathbb{T}^3} K_1 dx = K_1.$$

As mentioned in section 1.4, Rudnick and Wigman applied it to compute (1.4.8):

$$\mathbb{E}[\mathcal{A}] = \frac{4}{\sqrt{3}}\sqrt{m}.$$

We now turn to the nodal area variance. Recall that

$$\phi_{F(x),F(y)}$$

denotes the density of the Gaussian vector

$$(F(x), F(y)) \in \mathbb{R}^2,$$

and $\tilde{K_2} : \mathbb{T}^3 \times \mathbb{T}^3 \to \mathbb{R}$,

$$\tilde{K_2}(x) = \phi_{F(0),F(x)}(0,0) \cdot \mathbb{E}[\|\nabla F(0)\| \cdot \|\nabla F(x)\| \bigm| F(0) = F(x) = 0], \quad (5.4.1)$$

the two-point correlation function (2.4.16) of F, defined for $x \neq 0$.

Let us verify the hypotheses of Proposition 2.4.10, with $B = \mathbb{T}^3$, $P = F$, $j = 2$, $u_1 = u_2 = 0$, $t_1 = y$, and $t_2 = y + x$. The random field F is of course Gaussian, with smooth paths, while the condition (iv) is satisfied thanks to Lemma 5.4.1. To satisfy (iii)′, the covariance matrix

$$A = \begin{pmatrix} 1 & r_F(x,y) \\ r_F(x,y) & 1 \end{pmatrix}$$

of the Gaussian random vector $(F(x), F(y))$ must be positive definite for $x \neq y$ (recall r_F is the covariance function (5.1.1)). As F is stationary, it is equivalent to require

$$A = \begin{pmatrix} 1 & r_F(x) \\ r_F(x) & 1 \end{pmatrix}$$

to be positive definite for $x \neq 0$ (with the well-accepted abuse of notation). This condition holds except for finitely many points (e.g. the origin, and $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$), thanks to Proposition 2.4.7. Then (2.4.14) reads

$$\mathbb{E}(\mathcal{A}^2) = \int_{\mathbb{T}^3} \tilde{K_2}(x)dx. \quad (5.4.2)$$

It is more convenient to work with a scaled version of the second intensity,

$$K_2(x) := \frac{3}{E}\tilde{K_2}(x), \quad (5.4.3)$$

where we recall that $E = E_m = 4\pi^2 m$. Applying the Kac-Rice formulas, we obtain the following precise expression for the variance of the nodal area.

Proposition 5.4.2. *One has*

$$Var(\mathcal{A}) = \frac{E}{3}\int_{\mathbb{T}^3}\left(K_2(x) - \frac{4}{\pi^2}\right)dx. \tag{5.4.4}$$

Proof. By (5.4.2) and (1.2.11),

$$\begin{aligned}\mathbb{E}[\mathcal{A}^2] - (\mathbb{E}[\mathcal{A}])^2 &= \int_{\mathbb{T}^3}\tilde{K}_2(x)dx - \frac{16}{3}m = \int_{\mathbb{T}^3}\left(\tilde{K}_2(x) - \frac{16}{3}m\right)dx \\ &= \frac{E}{3}\int_{\mathbb{T}^3}\left(K_2(x) - \frac{3}{E}\frac{16}{3}m\right)dx = \frac{E}{3}\int_{\mathbb{T}^3}\left(K_2(x) - \frac{4}{\pi^2}\right)dx.\end{aligned}$$

□

A formula for K_2

By the arguments of section 5.4, to understand the nodal area variance of the arithmetic random wave F, we need to study the (scaled) two-point function K_2; let us begin by introducing the necessary notation. Recall the covariance function r of F is given by (5.1.1). Let

$$D(x) := \nabla r_F(x) = \frac{2\pi i}{\mathcal{N}}\sum_{\mu\in\mathcal{E}} e(\langle\mu, x\rangle)\cdot\mu, \tag{5.4.5}$$

where for $j = 1, 2, 3$ we have computed the partial derivatives

$$D_j(x) = \frac{\partial r}{\partial x_j}(x) = \frac{2\pi i}{\mathcal{N}}\sum_{\mu\in\mathcal{E}} e(\langle\mu, x\rangle)\mu^{(j)}, \qquad \mu = (\mu^{(1)}, \mu^{(2)}, \mu^{(3)}).$$

Further, denote

$$H(x) := -\frac{4\pi^2}{\mathcal{N}}\sum_{\mu\in\mathcal{E}} e(\langle\mu, x\rangle)\cdot\mu^t\mu \tag{5.4.6}$$

the Hessian 3×3 matrix of r, where for $j, k = 1, 2, 3$,

$$H_{jk}(x) := \frac{\partial^2 r_F}{\partial x_j\partial x_k}(x) = -\frac{4\pi^2}{\mathcal{N}}\sum_{\mu\in\mathcal{E}} e(\langle\mu, x\rangle)\mu^{(j)}\mu^{(k)}.$$

The $n\times n$ identity matrix will be denoted I_n.

Proposition 5.4.3. *The scaled two-point correlation function may be expressed as*

$$K_2(x) = \frac{1}{2\pi\sqrt{1-r_F^2(x)}} \cdot \mathbb{E}[\|w_1\| \cdot \|w_2\|], \tag{5.4.7}$$

where w_1, w_2 *are three-dimensional random vectors with Gaussian distribution* $(w_1, w_2) \sim N(0, \Omega(x))$*; their covariance matrix is given by*

$$\Omega = I_6 + \begin{pmatrix} X & Y \\ Y & X \end{pmatrix}, \tag{5.4.8}$$

the 3×3 *matrices* X *and* Y *being defined as*

$$X(x) = -\frac{1}{1-r_F^2}\frac{3}{E} \cdot D^t D \tag{5.4.9}$$

and

$$Y(x) = -\frac{3}{E} \cdot \left(H + \frac{r_F}{1-r_F^2} \cdot D^t D\right). \tag{5.4.10}$$

Proof. The first factor of the two-point function (5.4.1),

$$\tilde{K}_2(x) = \phi_{F(0),F(x)}(0,0) \cdot \mathbb{E}[\|\nabla F(0)\| \cdot \|\nabla F(x)\| \mid F(0) = F(x) = 0], \tag{5.4.11}$$

is the joint Gaussian density

$$\phi_{F(0),F(x)}(0,0) = \frac{1}{2\pi\sqrt{1-r_F^2(x)}}, \tag{5.4.12}$$

where we have used (2.4.1) and the expression

$$A(x) = \begin{pmatrix} 1 & r_F(x) \\ r_F(x) & 1 \end{pmatrix}, \tag{5.4.13}$$

for the covariance matrix of $(F(0), F(x))$. By [60, Lemma 5.1], the covariance matrix of the eight-dimensional Gaussian vector

$$(F(0), F(x), \nabla F(0), \nabla F(x))$$

is the block matrix $\Sigma(x) = \begin{pmatrix} A & B \\ B^t & C \end{pmatrix}$, with A as in (5.4.13),

$$B(x) = \begin{pmatrix} 0_{1\times 3} & D_{1\times 3}(x) \\ -D_{1\times 3}(x) & 0_{1\times 3} \end{pmatrix} \qquad \text{and} \qquad C = \begin{pmatrix} \frac{E}{3}I_3 & -H(x) \\ -H(x) & \frac{E}{3}I_3 \end{pmatrix}.$$

By Proposition 2.4.7, there are only finitely many $x \in \mathbb{T}^3$ such that $r_F(x) = \pm 1$. Therefore, for almost all $x \in \mathbb{T}^3$, the covariance matrix $A(x)$ is nonsingular. In view of [2, Proposition 1.2] (see also the hypotheses of Theorem 2.4.10), the covariance matrix of $(\nabla F(0), \nabla F(x))$ conditioned on $F(0) = 0, F(x) = 0$ is $\tilde{\Omega}(x) := C - B^t A^{-1} B$. We then have

$$\mathbb{E}[\|\nabla F(0)\| \cdot \|\nabla F(x)\| \bigm| F(0) = F(x) = 0] = \mathbb{E}[\|v_1\| \cdot \|v_2\|], \tag{5.4.14}$$

where v_1, v_2 are three-dimensional random vectors with $(v_1, v_2) \sim N(0, \tilde{\Omega})$. Inserting (5.4.12) and (5.4.14) into (5.4.11) we obtain

$$\tilde{K_2}(x) = \frac{1}{2\pi\sqrt{1 - r_F^2(x)}} \cdot \mathbb{E}[\|v_1\| \cdot \|v_2\|], \qquad (v_1, v_2) \sim N(0, \tilde{\Omega}). \tag{5.4.15}$$

Lastly, to prove the expression (5.4.7) for the scaled two-point function, we rescale the random vectors

$$v_i =: \sqrt{\frac{E}{3}} w_i \qquad i = 1, 2,$$

and the matrix

$$\tilde{\Omega} =: \frac{E}{3}\Omega;$$

then Ω is given by (5.4.8), with X, Y as in (5.4.9) and (5.4.10). □

In the proof of the latter proposition, we saw that the distribution of (w_1, w_2) is non-degenerate (i.e., the matrix $\Omega(x)$ is nonsingular) for almost all x. Also note that (5.4.8) expresses $\Omega(x)$ as a perturbation of the identity matrix, in the sense that the entries of $X(x), Y(x)$ are small for 'typical' $x \in \mathbb{T}^3$.

5.5 Nodal area variance: arithmetic formula

The contribution of the singular set

We will define a small subset of the torus, called the *singular set* S: outside of S, we will eventually establish precise asymptotics for the two-point correlation function K_2 (recall (5.4.3) and (5.4.1)). The goal of the present subsection is to bound K_2 on S, and also to control the measure of S. The definitions and results of the present section are borrowed from [54], [60] and [47]. Recall the notation $\mathcal{E}$ for the set of all lattice points on the sphere of radius $\sqrt{m}$.

Definition 5.5.1. We call the point $x \in \mathbb{T}^3$ *positive singular* (resp. *negative singular*) if there exists a subset $\mathcal{E}_x \subseteq \mathcal{E}$ with density $\frac{|\mathcal{E}_x|}{|\mathcal{E}|} > \frac{11}{12}$ such that $\cos(2\pi\langle\mu, x\rangle) > \frac{3}{4}$ (resp. $\cos(2\pi\langle\mu, x\rangle) < -\frac{3}{4}$) for all $\mu \in \mathcal{E}_x$.

For instance, the origin $(0, 0, 0)$ is a positive singular point. Take $q \asymp \sqrt{m}$ and partition the torus into q^3 cubes, each centred at a/q, $a \in \mathbb{Z}^3$, of side length $1/q$. Note that the cubes have disjoint interiors.

Definition 5.5.2. We call the cube $Q \subset \mathbb{T}^3$ *positive singular* (resp. *negative singular*) if it contains a positive (resp. negative) singular point.

Definition 5.5.3. The **singular set** S is the union of all positive and negative singular cubes.

The main result of the present subsection is the bound for the integral of K_2 on S, for which we shall need two lemmas. The covariance function r of the arithmetic random wave F satisfies $|r(x)| \leq 1$. The following lemma shows that, on S, r is bounded away from 0.

Lemma 5.5.4 ([54, Lemmas 6.4 and 6.5])**.**

1. *For all positive (resp. negative) singular cubes Q, there exists a subset $\mathcal{E}_Q \subseteq \mathcal{E}$ with density $\frac{|\mathcal{E}_x|}{|\mathcal{E}|} > \frac{11}{12}$ such that for all $y \in Q$ and for all $\mu \in \mathcal{E}_Q$, we have*
$$\cos(2\pi\langle\mu, y\rangle) > \frac{1}{2}$$
(resp. $\cos(2\pi\langle\mu, y\rangle) < -1/2$*).*

2. *For all $y \in S$:*
$$|r(y)| > \frac{3}{8}.$$

Recall the definitions (5.4.9) and (5.4.10) for the matrices $X(x)$ and $Y(x)$.

Lemma 5.5.5 (cf. [47, Lemma 3.2])**.** *We have uniformly (entry-wise)*

$$X(x) = O(1), \quad Y(x) = O(1). \tag{5.5.1}$$

One immediate consequence is

$$K_2(x) \ll \frac{1}{\sqrt{1 - r_F^2(x)}}. \tag{5.5.2}$$

Recall the notation $\mathcal{R}(\ell)$ (2.4.7) for the ℓ-th moment of the covariance function r_F.

Proposition 5.5.6 (cf. [54, section 6.3] and [47, Lemma 4.4])**.**

1. *The contribution of the singular set to* (5.4.4) *has the following bound:*
$$\int_S |K_2(x)| dx \ll meas(S),$$
where 'meas' is Lebesgue measure.

2. *For all integers $\ell \geq 0$:*
$$meas(S) \ll \mathcal{R}(\ell).$$

We end this subsection with a property of the covariance function outside the singular set.

Lemma 5.5.7 ([54, Lemma 6.5]). *For all $x \notin S$, $|r(x)|$ is bounded away from 1:*

$$|r_F(x)| \le 1 - \frac{1}{48}.$$

Thanks to the lemma, on the non-singular set $\mathbb{T}^3 \setminus S$ we have the following approximations:

$$\frac{1}{\sqrt{1-r_F^2}} = 1 + \frac{1}{2}r_F^2 + \frac{3}{8}r_F^4 + O(r_F^6) \tag{5.5.3}$$

and

$$\frac{1}{1-r_F^2} = 1 + r_F^2 + O(r_F^4). \tag{5.5.4}$$

Asymptotics for K_2 on the non-singular set

Lemma 5.5.8. *Let $(w_1, w_2) \sim N(0, \Omega)$, $\Omega = I_6 + \begin{pmatrix} X & Y \\ Y & X \end{pmatrix}$, with rank$(X) = 1$. Then:*

$$\mathbb{E}[\|w_1\| \cdot \|w_2\|] = \frac{8}{\pi} \cdot \left[1 + \frac{tr(X)}{3} + \frac{tr(Y^2)}{18} - \frac{tr(XY^2)}{45} - \frac{tr(X^2)}{45} + \frac{tr(Y^4)}{900} + \frac{tr(Y^2)^2}{1800} - \frac{tr(X)tr(Y^2)}{90}\right] + O(tr(X^3) + tr(Y^6)).$$

The proof of Lemma 5.5.8 is quite lengthy and takes up the whole of appendix C. Assuming it, we arrive at the asymptotics for K_2 on $\mathbb{T}^3 \setminus S$.

Proposition 5.5.9. *For $x \in \mathbb{T}^3$ such that $r(x)$ is bounded away from ± 1, we have the following asymptotics for the (scaled) two point correlation function:*

$$K_2(x) = \frac{4}{\pi^2} + L_2(x) + \epsilon(x)$$

where

$$L_2(x) := \frac{4}{\pi^2}\left[\frac{1}{2}r^2 + \frac{tr(X)}{3} + \frac{tr(Y^2)}{18} + \frac{3}{8}r^4 - \frac{tr(XY^2)}{45} - \frac{tr(X^2)}{45} + \frac{tr(Y^4)}{900} + \frac{tr(Y^2)^2}{1800} - \frac{tr(X)tr(Y^2)}{90} + \frac{1}{6}r^2 tr(X) + \frac{1}{36}r^2 tr(Y^2)\right] \tag{5.5.5}$$

and

$$\epsilon(x) := O[r^6 + tr(X^3) + tr(Y^6)].$$

Proof of Proposition 5.5.9 assuming Lemma 5.5.8. By Proposition 5.4.3, we have (5.4.7); for the first factor of (5.4.7), as $r_F(x)$ is bounded away from ± 1, we may use the expansion (5.5.3). On the second factor of (5.4.7), apply Lemma 5.5.8 with X, Y as in (5.4.9) and (5.4.10). □

Later we will need to integrate L_2 term-wise, using the following lemma.

Lemma 5.5.10. *We have the following estimates:*

1.
$$\int_{\mathbb{T}^3} trX(x)dx = -\frac{3}{\mathcal{N}} - \frac{3}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

2.
$$\int_{\mathbb{T}^3} trY^2(x)dx = \frac{9}{\mathcal{N}} - \frac{6}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

3.
$$\int_{\mathbb{T}^3} tr(XY^2)(x)dx = -\frac{9}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

4.
$$\int_{\mathbb{T}^3} tr(X^2)(x)dx = \frac{15}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

5.
$$\int_{\mathbb{T}^3} tr(Y^4)(x)dx = \frac{351}{5} \cdot \frac{1}{\mathcal{N}^2} + O\left(\frac{1}{m^{1/28-o(1)} \cdot \mathcal{N}^2} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

6.
$$\int_{\mathbb{T}^3} (trY^2(x))^2dx = \frac{567}{5} \cdot \frac{1}{\mathcal{N}^2} + O\left(\frac{1}{m^{1/28-o(1)} \cdot \mathcal{N}^2} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

7.
$$\int_{\mathbb{T}^3} (trX \cdot trY^2)(x)dx = -\frac{27}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

8.
$$\int_{\mathbb{T}^3}(r_F^2 trX)(x)dx = -\frac{3}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

9.
$$\int_{\mathbb{T}^3}(r_F^2 tr(Y^2))(x)dx = \frac{15}{\mathcal{N}^2} + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

10.
$$\int_{\mathbb{T}^3} tr(X^3)(x)dx = O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

11.
$$\int_{\mathbb{T}^3} tr(Y^6)(x)dx = O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

The proof of Lemma 5.5.10 is given in section 5.6.

Proof of Proposition 1.4.2

Assuming the above preparatory results, we arrive at the asymptotics for the nodal area variance.

Proof of Proposition 1.4.2. In the expression for the variance of Proposition 5.4.2, we separate the domain of integration over the singular set $S \subset \mathbb{T}^3$ of Definition 5.5.3 and its complement:

$$Var(\mathcal{A}) = \frac{E}{3}\int_{\mathbb{T}^3\setminus S}\left(K_2(x) - \frac{4}{\pi^2}\right)dx + \frac{E}{3}\int_S\left(K_2(x) - \frac{4}{\pi^2}\right)dx. \tag{5.5.6}$$

By Lemma 5.5.7, the asymptotics for K_2 of Proposition 5.5.9 hold outside the singular set:

$$\int_{\mathbb{T}^3\setminus S}\left(K_2(x) - \frac{4}{\pi^2}\right)dx = \int_{\mathbb{T}^3\setminus S} L_2(x)dx + O\int_{\mathbb{T}^3\setminus S}|\epsilon(x)|dx. \tag{5.5.7}$$

Note that the constant term $4/\pi^2$ of the nodal area variance cancels out with the expectation squared. Next, recall Proposition 5.5.6:

$$\int_S |K_2(x)|dx \ll meas(S) \ll \mathcal{R}(6) = \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}. \tag{5.5.8}$$

Inserting (5.5.7) and (5.5.8) into (5.5.6) gives

$$Var(\mathcal{A}) = \frac{E}{3}\int_{\mathbb{T}^3\setminus S} L_2(x)dx + E\left(O\left(\int_{\mathbb{T}^3\setminus S}|\epsilon(x)|dx\right)+O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right)\right). \quad (5.5.9)$$

The former error term is redundant by Lemma 5.5.10, parts 10 and 11. Using $|r_F(x)| \leq 1$ and Lemma 5.5.5 in the expression (5.5.5) for L_2, we get

$$\left|\int_{\mathbb{T}^3\setminus S} L_2(x)dx - \int_{\mathbb{T}^3} L_2(x)dx\right| \ll \int_S |L_2(x)|dx \ll meas(S)$$

which together with (5.5.9) and (5.5.8) implies

$$Var(\mathcal{A}) = \frac{E}{3}\int_{\mathbb{T}^3} L_2(x)dx + O\left(E\cdot\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right). \quad (5.5.10)$$

We integrate (5.5.10) term-wise (recall the expression (5.5.5) for L_2), and, as the integral is over the whole torus, we may apply the considerations

$$\int_{\mathbb{T}^3} r_F^2(x)dx = \frac{1}{\mathcal{N}}, \qquad \int_{\mathbb{T}^3} r_F^4(x)dx = \frac{3}{\mathcal{N}^2} + O\left(\frac{1}{\mathcal{N}^3}+\frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right)$$

(see Lemma 5.6.1), and the estimates of Lemma 5.5.10, to deduce:

$$\begin{aligned}
\mathrm{Var}(\mathcal{A}) = \frac{E}{3}\frac{4}{\pi^2}\int_{\mathbb{T}^3}&\left[\frac{1}{2}r_F^2 + \frac{tr(X)}{3} + \frac{tr(Y^2)}{18} + \frac{3}{8}r_F^4 - \frac{tr(XY^2)}{45} - \frac{tr(X^2)}{45} + \frac{tr(Y^4)}{900}\right.\\
&\left.+\frac{tr(Y^2)^2}{1800} - \frac{tr(X)tr(Y^2)}{90} + \frac{1}{6}r^2tr(X) + \frac{1}{36}r^2tr(Y^2)\right]dx + O\left(E\cdot\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right)\\
= \frac{E}{3}\frac{4}{\pi^2}&\left[\frac{1}{\mathcal{N}}\left(\frac{1}{2}-\frac{1}{3}\cdot(-3)+\frac{1}{18}\cdot 9\right)\right.\\
&+\frac{1}{\mathcal{N}^2}\left(\frac{1}{3}\cdot(-3)+\frac{1}{18}\cdot(-6)+\frac{3}{8}\cdot 3-\frac{1}{45}(-9)-\frac{1}{45}\cdot 15+\frac{1}{900}\cdot\frac{351}{5}\right.\\
&\left.+\frac{1}{1800}\cdot\frac{567}{5}-\frac{1}{90}(-27)+\frac{1}{6}(-3)+\frac{1}{36}\cdot 15\right)\\
&\left.+O\left(\frac{1}{m^{1/28-o(1)}\cdot\mathcal{N}^2}+\frac{|\mathcal{X}(4)|}{\mathcal{N}^4}+\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right)\right],
\end{aligned}$$

where we note the error term $m/\mathcal{N}^3$ is negligible. The terms of order $m/\mathcal{N}$ cancel perfectly: as noted in section 1.4, the 3-dimensional torus exhibits arithmetic

Berry cancellation (see the next section for more details). The terms of order $m/\mathcal{N}^2$ sum up to

$$\frac{E}{3}\cdot\frac{4}{\pi^2}\cdot\frac{1}{\mathcal{N}^2}\cdot\frac{6}{375}=\frac{32}{375}\cdot\frac{m}{\mathcal{N}^2},$$

hence, recalling (1.3.5), the claim of the present proposition. $\square$

A note on arithmetic Berry cancellation

Let us analyse in more detail the vanishing of the term of order $m/\mathcal{N}$ of the nodal area variance (cf. [47, section 4.2]). The leading term of $K_2(x)-4/\pi^2$ is (recall (5.5.5), (5.4.9) and (5.4.10))

$$\begin{aligned}\frac{4}{\pi^2}\left[\frac{1}{2}r_F^2+\frac{tr(X)}{3}+\frac{tr(Y^2)}{18}\right]&\sim\frac{4}{\pi^2}\left[\frac{1}{2}r_F^2+\frac{1}{3}\left(\frac{3}{E}DD^t\right)+\frac{1}{18}\left(\frac{9}{E^2}tr(H^2)\right)\right]\\&=\frac{2}{\pi^2}v(x),\end{aligned}$$

having defined

$$v(x):=r_F^2(x)-\frac{2}{E}(DD^t)(x)+\frac{1}{E^2}tr(H^2(x)).$$

The latter expression has the same shape as the two-dimensional case [47, (39)]: the remainder of this discussion is essentially identical to [47, section 4.2]. One rewrites

$$v(x)=\frac{4}{N^2}\sum_{\mu_1,\mu_2\in\mathcal{E}}e\langle(\mu_1+\mu_2),x\rangle\cdot\cos^4\left(\frac{\varphi_{\mu_1,\mu_2}}{2}\right),$$

where φ_{μ_1,μ_2} is the angle between the two lattice points μ_1,μ_2. On integrating over the torus (5.4.4), all summands such that $\mu_1+\mu_2\neq 0$ vanish (see also (5.6.1) to follow). As $\varphi_{\mu_1,-\mu_1}=\pi$, the arithmetic cancellation phenomenon is tantamount to $\cos^4(\varphi/2)$ vanishing at π, similarly to the two-dimensional problem.

5.6 The leading term of the variance

Preparatory results

Recall the expression of the covariance function (5.1.1) and its derivatives (5.4.5) and (5.4.6); also recall the notation of Definition 2.2.14 for the set of lattice point correlations.

Lemma 5.6.1. *We have the following estimates:*

1.
$$\int_{\mathbb{T}^3} r_F^2(x)dx = \frac{1}{\mathcal{N}};$$
$$\int_{\mathbb{T}^3} r_F^4(x)dx = \frac{3}{\mathcal{N}^2} + O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

2.
$$\frac{1}{E}\int_{\mathbb{T}^3} (DD^t)(x)dx = \frac{1}{\mathcal{N}};$$
$$\frac{1}{E^2}\int_{\mathbb{T}^3} (DD^t)^2(x)dx = \frac{5}{3}\cdot\frac{1}{\mathcal{N}^2} + O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

3.
$$\frac{1}{E}\int_{\mathbb{T}^3} (r_F^2 DD^t)(x)dx = \frac{1}{\mathcal{N}^2} + O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

4.
$$\frac{1}{E^2}\int_{\mathbb{T}^3} tr(H^2(x))dx = \frac{1}{\mathcal{N}};$$
$$\frac{1}{E^2}\int_{\mathbb{T}^3} (r_F^2 tr(H^2))(x)dx = \frac{5}{3}\cdot\frac{1}{\mathcal{N}^2} + O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

5.
$$\frac{1}{E^4}\int_{\mathbb{T}^3} tr(H^4(x))dx = \frac{13}{15}\cdot\frac{1}{\mathcal{N}^2} + O\left(\frac{1}{m^{1/28-o(1)}\cdot\mathcal{N}^2} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right);$$
$$\frac{1}{E^4}\int_{\mathbb{T}^3} tr(H^2(x))^2dx = \frac{7}{5}\cdot\frac{1}{\mathcal{N}^2} + O\left(\frac{1}{m^{1/28-o(1)}\cdot\mathcal{N}^2} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

6.
$$\frac{1}{E^3}\int_{\mathbb{T}^3}(DD^t tr(H^2))(x)dx=\frac{1}{\mathcal{N}^2}+O\left(\frac{1}{\mathcal{N}^3}+\frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

7.
$$\frac{1}{E^2}\int_{\mathbb{T}^3}(r_F DHD^t)(x)dx=-\frac{1}{3}\cdot\frac{1}{\mathcal{N}^2}+O\left(\frac{1}{\mathcal{N}^3}+\frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

8.
$$\frac{1}{E^3}\int_{\mathbb{T}^3}(DH^2D^t)(x)dx=\frac{1}{3}\cdot\frac{1}{\mathcal{N}^2}+O\left(\frac{1}{\mathcal{N}^3}+\frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

9.
$$\frac{1}{E^3}\int_{\mathbb{T}^3}(DD^t)^3(x)dx\ll\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}.$$

10.
$$\frac{1}{E}\int_{\mathbb{T}^3}(r_F^4 DD^t)(x)dx\ll\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}.$$

11.
$$\frac{1}{E^6}\int_{\mathbb{T}^3}tr(H^6(x))dx\ll\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}.$$

12.
$$\frac{1}{E^3}\int_{\mathbb{T}^3}(r_F DD^t DHD^t)(x)dx\ll\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}.$$

Proof. The various estimates are obtained with the following common strategy. Firstly, one rewrites the integrand using the expressions (5.1.1), (5.4.5) and (5.4.6) for the covariance function and its (first and second order) derivatives. Next, the integral over the torus in taken, invoking the orthogonality relations of the exponentials:

$$\int_{\mathbb{T}^3}e(\langle\mu,x\rangle)dx=\begin{cases}1 & \mu=0\\ 0 & \mu\neq 0.\end{cases}\tag{5.6.1}$$

We are thus left with a summation over the set of ℓ-correlations $\mathcal{C}(\ell)$, where $\ell=2,4$ or 6. The summands are certain products of inner products between two lattice points. The summations involving 2-correlations are computed directly, and for $k = 6$ we need only an upper bound. The most delicate computations are for 4-correlations, when we split the summation exploiting the structure of $\mathcal{C}(4)$ (see (5.2.4)). This leads to computing k-th moments (for $k = 1, 2, 3$, or 4) of the normalised inner product of two lattice points, applying Lemma 2.2.13.

We now present the details of the proof for some of the estimates of the present lemma; the remaining computations apply the same ideas (outlined above), and we will omit them here. We begin with part 1, first statement, which is an immediate consequence of (2.2.17):

$$\int_{\mathbb{T}^3} r_F^2(x)dx = \mathcal{R}(2) = \frac{|\mathcal{C}(2)|}{\mathcal{N}^2} = \frac{1}{\mathcal{N}}.$$

The second statement of part 1 follows from the structure of $\mathcal{C}(4)$ (5.2.4):

$$\int_{\mathbb{T}^3} r_F^4(x)dx = \mathcal{R}(4) = \frac{|\mathcal{C}(4)|}{\mathcal{N}^4} = \frac{3}{\mathcal{N}^2} + O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

Let us show part 2 of the present lemma, starting with the first statement. By (5.4.5), we may rewrite the integrand as

$$DD^t = tr(D^tD) = -\frac{4\pi^2}{\mathcal{N}^2} \cdot \sum_{\mu_1,\mu_2} e\langle(\mu_1 + \mu_2), x\rangle\langle\mu_1, \mu_2\rangle. \tag{5.6.2}$$

We take the integral over $\mathbb{T}^3$, bearing in mind (5.6.1), and compute the resulting summation over the set of 2-correlations, using (2.2.17):

$$\int_{\mathbb{T}^3}(DD^t)(x)dx = -\frac{4\pi^2}{\mathcal{N}^2} \cdot \sum_{\mathcal{C}(2)}\langle\mu_1, \mu_2\rangle = -\frac{4\pi^2}{\mathcal{N}^2} \cdot \sum_{\mu_2}\langle-\mu_2, \mu_2\rangle = \frac{E}{\mathcal{N}},$$

as claimed. For the second statement of part 2, we begin by squaring (5.6.2):

$$(DD^t)^2 = \frac{(4\pi^2)^2}{\mathcal{N}^4} \cdot \sum_{\mathcal{E}_m^4} e\langle(\mu_1 + \mu_2 + \mu_3 + \mu_4), x\rangle \cdot \langle\mu_1, \mu_2\rangle \cdot \langle\mu_3, \mu_4\rangle.$$

By (5.6.1),

$$\int_{\mathbb{T}^3}(DD^t)^2dx = \frac{(4\pi^2)^2}{\mathcal{N}^4} \cdot \sum_{\mathcal{C}(4)}\langle\mu_1, \mu_2\rangle \cdot \langle\mu_3, \mu_4\rangle. \tag{5.6.3}$$

To treat the resulting summation over 4-correlations, we split it with (5.2.4). The contribution over diagonal and non-degenerate quadruples is bounded via Cauchy-Schwartz:

$$\sum_{\mathcal{D}''\dot\cup\mathcal{X}(4)} \langle\mu_1,\mu_2\rangle\cdot\langle\mu_3,\mu_4\rangle \leq \sum_{\mathcal{D}''\dot\cup\mathcal{X}(4)} (\sqrt{m})^4 \ll m^2\cdot(\mathcal{N}+|\mathcal{X}(4)|).$$

There are three more contributions to the summation in (5.6.3), that arise from symmetric (and non-diagonal) 4-correlations; we directly compute the first of these contributions:

$$\sum_{\substack{\mu_1=-\mu_2\\ \mu_3=-\mu_4}} \langle\mu_1,\mu_2\rangle\cdot\langle\mu_3,\mu_4\rangle = \sum_{\mu_2,\mu_4}\langle-\mu_2,\mu_2\rangle\cdot\langle-\mu_4,\mu_4\rangle = m^2\mathcal{N}^2.$$

For the remaining two summations, we invoke Lemma 2.2.13 with $k=2$:

$$\sum_{\substack{\mu_1=-\mu_3\\ \mu_2=-\mu_4}} \langle\mu_1,\mu_2\rangle\cdot\langle\mu_3,\mu_4\rangle = \sum_{\substack{\mu_1=-\mu_4\\ \mu_2=-\mu_3}} \langle\mu_1,\mu_2\rangle\cdot\langle\mu_3,\mu_4\rangle = \sum_{\mu_4}\sum_{\mu_3}\langle\mu_3,\mu_4\rangle^2 = \frac{m^2\mathcal{N}^2}{3}.$$

The various contributions yield

$$\sum_{\mathcal{C}(4)}\langle\mu_1,\mu_2\rangle\cdot\langle\mu_3,\mu_4\rangle = \frac{5}{3}\cdot m^2\mathcal{N}^2 + O(m^2\mathcal{N}) + O(m^2\cdot|\mathcal{X}(4)|). \tag{5.6.4}$$

Inserting (5.6.4) into (5.6.3) we arrive at the second statement of part 2 of the present lemma. The proof of part 3 is very similar to that of part 2, second statement, except Lemma 2.2.13 is applied with $k=1$.

To prove part 4, first statement, recall (5.4.6) and (5.6.1) to directly compute

$$\int_{\mathbb{T}^3} tr(H^2(x))dx = \frac{(4\pi^2)^2}{\mathcal{N}^2}\cdot\sum_{\mathcal{C}(2)} tr(\mu_1^t\mu_1\mu_2^t\mu_2) = \frac{(4\pi^2)^2}{\mathcal{N}^2}\cdot\sum_{\mu_1}\langle\mu_1,\mu_1\rangle^2 = \frac{E^2}{\mathcal{N}}.$$

For part 4, second statement, (5.1.1), (5.4.6) and (5.6.1) imply

$$\int_{\mathbb{T}^3}(r_F^2 tr(H^2))(x)dx = \frac{(4\pi^2)^2}{\mathcal{N}^4}\cdot\sum_{\mathcal{C}(4)} tr({\mu_3}^t\mu_3{\mu_4}^t\mu_4) = \frac{(4\pi^2)^2}{\mathcal{N}^4}\cdot\sum_{\mathcal{C}(4)}\langle\mu_3,\mu_4\rangle^2;$$

one now splits the sum and proceeds as in the proof of part 2.

Let us prove part 5 of the present lemma, first statement. By (5.4.6) and (5.6.1), we have

$$\int_{\mathbb{T}^3} tr(H^4(x))dx = \frac{(4\pi^2)^4}{\mathcal{N}^4} \sum_{\mathcal{C}(4)} tr(\mu_1{}^t\mu_1\mu_2{}^t\mu_2\mu_3{}^t\mu_3\mu_4{}^t\mu_4)$$
$$= \frac{(4\pi^2)^4}{\mathcal{N}^4} \left[\sum_{\mu_2,\mu_4} tr(\mu_2{}^t\mu_2\mu_2{}^t\mu_2\mu_4{}^t\mu_4\mu_4{}^t\mu_4) + \sum_{\mu_3,\mu_4} tr(\mu_3{}^t\mu_3\mu_4{}^t\mu_4\mu_3{}^t\mu_3\mu_4{}^t\mu_4)\right.$$
$$\left. + \sum_{\mu_3,\mu_4} tr(\mu_4{}^t\mu_4\mu_3{}^t\mu_3\mu_3{}^t\mu_3\mu_4{}^t\mu_4)\right] + E^4 \cdot O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right)$$
$$= \frac{(4\pi^2)^4}{\mathcal{N}^4} \left[\sum_{\mu_2,\mu_4} m^2\langle\mu_2,\mu_4\rangle^2 + \sum_{\mu_3,\mu_4} \langle\mu_3,\mu_4\rangle^4 + \sum_{\mu_3,\mu_4} m^2\langle\mu_3,\mu_4\rangle^2\right]$$
$$+ E^4 \cdot O\left(\frac{1}{\mathcal{N}^3} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4}\right).$$

One computes the three summations on the RHS of the latter expression via Lemma 2.2.13, with $k = 2, 4$:

$$\int_{\mathbb{T}^3} tr(H^4(x))dx = \frac{E^4}{\mathcal{N}^2}\left[\frac{1}{3} + \frac{1}{5} + \frac{1}{3} + O\left(\frac{1}{m^{1/28-o(1)}}\right) + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^2}\right)\right],$$

where we note the error term $E^4/\mathcal{N}^3$ is negligible by (1.3.5). The second statement of part 5, and parts 6, 7 and 8 of the present lemma are all derived in a similar fashion, and we will omit these proofs here.

Let us prove part 12 of the present lemma, parts 9, 10 and 11 being similar. By (5.1.1), (5.4.5), (5.4.6) and (5.6.1),

$$\int_{\mathbb{T}^3} (r_F DD^t DHD^t)(x)dx = -\frac{(4\pi^2)^3}{\mathcal{N}^6} \sum_{\mathcal{C}(6)} \langle\mu_1,\mu_2\rangle \cdot \langle\mu_3,\mu_4\rangle \cdot \langle\mu_4,\mu_5\rangle \ll \frac{E^3}{\mathcal{N}^6} \cdot |\mathcal{C}(6)|$$

(for summations over 6-correlations, an upper bound via the Cauchy-Schwartz inequality is sufficient for our purposes). $\square$

Proof of Lemma 5.5.10

Proof of Lemma 5.5.10. To prove part 1, recall Lemma 5.5.5 (uniform boundedness of X) and write

$$\int_{\mathbb{T}^3} trX(x)dx = \int_{\mathbb{T}^3\setminus S} trX(x)dx + O(meas\ S).$$

Recall the expression of X (5.4.9); one uses the approximation (5.5.4) on $\mathbb{T}^3 \setminus S$, and Proposition 5.5.6 to bound the contribution of the singular set:

$$\int_{\mathbb{T}^3} trX(x)dx = -\frac{3}{E}\left(\int_{\mathbb{T}^3} DD^t dx + \int_{\mathbb{T}^3} r_F^2 DD^t dx\right) + O\left(\frac{1}{E}\int_{\mathbb{T}^3} r_F^4 DD^t dx\right) + O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

To compute the three integrals on the RHS of the latter expression, apply Lemma 5.6.1, parts 2, 3 and 10. Here and elsewhere the error term $1/\mathcal{N}^3$ (arising from several of the estimates of Lemma 5.6.1) is negligible compared to $|\mathcal{C}(6)|/\mathcal{N}^6$. Part 2 of the present lemma is derived in a similar way.

Let us show part 3 of the present lemma, parts 4, 7, 8 and 9 being similar. By Lemma 5.5.5, (5.5.4) and Proposition 5.5.6,

$$\int_{\mathbb{T}^3} tr(XY^2)(x)dx = -\frac{27}{E^3}\left[\int_{\mathbb{T}^3} tr(DH^2D^t)dx + O\int_{\mathbb{T}^3} r_F DD^t DHD^t dx\right] + O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

In light of Lemma 5.6.1, parts 8 and 12,

$$\int_{\mathbb{T}^3} tr(XY^2)(x)dx = \frac{1}{\mathcal{N}^2}\left[-9 + O\left(\frac{|\mathcal{X}(4)|}{\mathcal{N}^2} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^4}\right)\right],$$

which concludes the proof of part 3 of the present lemma.

We now prove part 5, part 6 being similar. By Lemma 5.5.5 and Proposition 5.5.6, we have

$$\int_{\mathbb{T}^3} tr(Y^4)(x)dx = \frac{81}{E^4}\int_{\mathbb{T}^3} tr(H^4)dx + O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right).$$

Now Lemma 5.6.1, part 5 yields

$$\int_{\mathbb{T}^3} tr(Y^4)(x)dx = \frac{351}{5} \cdot \frac{1}{\mathcal{N}^2} + O\left(\frac{1}{m^{1/28-o(1)} \cdot \mathcal{N}^2} + \frac{|\mathcal{X}(4)|}{\mathcal{N}^4} + \frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right),$$

hence the claim of part 5 of the present lemma.

Lastly, we show part 10, part 11 being similar. By Lemma 5.5.5 and Proposition 5.5.6, we have

$$\int_{\mathbb{T}^3} tr(X^3)(x)dx = -\frac{27}{E^3} \int_{\mathbb{T}^3} (DD^t)^3(x)dx + O\left(\frac{|\mathcal{C}(6)|}{\mathcal{N}^6}\right) \ll \frac{|\mathcal{C}(6)|}{\mathcal{N}^6},$$

where in the last step we applied Lemma 5.6.1, part 9. $\square$

Appendix A

The second moment of r and of its derivatives

In this appendix we prove Proposition 3.3.2, for which we need two auxiliary lemmas. We will work on the two-dimensional torus, though the argument extends almost verbatim to higher dimensions. Recall that $r = r(t_1, t_2)$ is the covariance function of the arithmetic random wave F restricted to a straight line segment $\mathcal{C}$, and the notation

$$r_1 = \frac{\partial r(t_1,t_2)}{\partial t_1}, \qquad r_2 = \frac{\partial r(t_1,t_2)}{\partial t_2} \qquad \text{and} \quad r_{12} = \frac{\partial^2 r(t_1,t_2)}{\partial t_1 \partial t_2}$$

for the derivatives of r. Also recall (3.2.4):

$$\mathfrak{R}_2(m) := \int_0^L \int_0^L \left(r^2 + \left(\frac{r_1}{\sqrt{m}}\right)^2 + \left(\frac{r_2}{\sqrt{m}}\right)^2 + \left(\frac{r_{12}}{m}\right)^2 \right) dt_1 dt_2.$$

As stated previously, the following lemma generalises readily to higher dimensions, c.f. Lemma 4.3.1 for dimension 3.

Lemma A.1.1. *Let $\mathcal{C}$ be a straight line segment. Then*

$$\mathfrak{R}_2(m) \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2.$$

Proof. We will show

$$\int_0^L \int_0^L r^2(t_1,t_2)dt_1dt_2 \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2, \tag{A.1.1}$$

$$\int_0^L \int_0^L \left(\frac{r_i(t_1,t_2)}{\sqrt{m}}\right)^2 dt_1dt_2 \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2, \tag{A.1.2}$$

for $i = 1, 2$, and

$$\int_0^L \int_0^L \left(\frac{r_{12}(t_1,t_2)}{m}\right)^2 dt_1dt_2 \ll \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2. \tag{A.1.3}$$

We begin by squaring the covariance function (2.4.6):

$$|r|^2 = \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} e^{2\pi i(t_1-t_2)\langle \mu-\mu',\alpha\rangle}$$

so that

$$\int_0^L \int_0^L |r(t_1,t_2)|^2 dt_1dt_2 = \int_0^L \int_0^L \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} e^{2\pi i(t_1-t_2)\langle \mu-\mu',\alpha\rangle} dt_1dt_2$$
$$= \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \int_0^L e^{2\pi i t_1\langle \mu-\mu',\alpha\rangle} dt_1 \int_0^L e^{-2\pi i t_2\langle \mu-\mu',\alpha\rangle} dt_2$$
$$= \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle \mu-\mu',\alpha\rangle} dt \right|^2,$$

yielding (A.1.1). Next,

$$r_1 = \frac{\partial r(t_1,t_2)}{\partial t_1} = \frac{1}{\mathcal{N}} \sum_{\mu\in\mathcal{E}} 2\pi i\langle \mu,\alpha\rangle e^{2\pi i(t_1-t_2)\langle \mu,\alpha\rangle}$$

and it follows that

$$\frac{r_1}{2\pi i\sqrt{m}} = \frac{1}{\mathcal{N}} \sum_{\mu\in\mathcal{E}} \left\langle \frac{\mu}{\|\mu\|}, \alpha \right\rangle e^{2\pi i(t_1-t_2)\langle \mu,\alpha\rangle}.$$

By Cauchy-Schwartz,

$$\begin{aligned}
&\int_0^L \int_0^L \left|\frac{r_1}{2\pi\sqrt{m}}\right|^2 dt_1 dt_2 \\
&= \int_0^L \int_0^L \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left\langle \frac{\mu}{\|\mu\|}, \alpha \right\rangle \left\langle \frac{\mu'}{\|\mu'\|}, \alpha \right\rangle e^{2\pi i(t_1-t_2)\langle\mu,\alpha\rangle} e^{2\pi i(t_1-t_2)\langle\mu',\alpha\rangle} dt_1 dt_2 \\
&\leq \int_0^L \int_0^L \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} e^{2\pi i(t_1-t_2)\langle\mu,\alpha\rangle} e^{2\pi i(t_1-t_2)\langle\mu',\alpha\rangle} dt_1 dt_2 \\
&= \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \int_0^L e^{2\pi i t_1\langle\mu-\mu',\alpha\rangle} dt_1 \int_0^L e^{-2\pi i t_2\langle\mu-\mu',\alpha\rangle} dt_2 \\
&= \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle\mu-\mu',\alpha\rangle} dt \right|^2
\end{aligned}$$

and (A.1.2) follows.

For the second mixed derivative:

$$r_{12} = \frac{\partial^2 r(t_1,t_2)}{\partial t_1 \partial t_2} = \frac{1}{\mathcal{N}} \sum_{\mu\in\mathcal{E}} (2\pi i)^2 \langle\mu,\alpha\rangle^2 e^{2\pi i(t_1-t_2)\langle\mu,\alpha\rangle}$$

thus

$$-\frac{r_{12}}{4\pi^2 m} = \frac{1}{\mathcal{N}} \sum_{\mu\in\mathcal{E}} \left\langle \frac{\mu}{\|\mu\|}, \alpha \right\rangle^2 e^{2\pi i(t_1-t_2)\langle\mu,\alpha\rangle}.$$

Again by Cauchy-Schwartz,

$$\begin{aligned}
&\int_0^L \int_0^L \left|\frac{r_{12}}{4\pi^2 m}\right|^2 dt_1 dt_2 \\
&= \int_0^L \int_0^L \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left\langle \frac{\mu}{\|\mu\|}, \alpha \right\rangle^2 \left\langle \frac{\mu'}{\|\mu'\|}, \alpha \right\rangle^2 e^{2\pi i(t_1-t_2)\langle\mu,\alpha\rangle} e^{2\pi i(t_1-t_2)\langle\mu',\alpha\rangle} dt_1 dt_2 \\
&\leq \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu')\in\mathcal{E}^2} \left| \int_0^L e^{2\pi i t\langle\mu-\mu',\alpha\rangle} dt \right|^2,
\end{aligned}$$

yielding (A.1.3). $\square$

Lemma A.1.2. *We have the following bound:*

$$\sum_{(\mu,\mu')\in\mathcal{E}^2}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 \ll \mathcal{N}+\sum_{A_\alpha}\min\left(1,\frac{1}{\langle\mu-\mu',\alpha\rangle^2}\right).$$

Proof. We split the summation over three ranges: diagonal pairs, off-diagonal pairs satisfying $\mu-\mu'\perp\alpha$, and the set A_α of Definition 3.3.1:

$$\sum_{(\mu,\mu')\in\mathcal{E}^2}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 = \sum_{\mu=\mu'}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 + \sum_{\substack{\mu\neq\mu'\\ \mu-\mu'\perp\alpha}}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 + \sum_{A_\alpha}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2. \tag{A.1.4}$$

The sum for $\mu=\mu'$ contains $\mathcal{N}$ summands (cf. [61], section 5):

$$\sum_{\mu=\mu'}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 = \sum_{\mu}L^2 = L^2\cdot\mathcal{N}. \tag{A.1.5}$$

By "Zygmund's trick" [74], there can be at most $\mathcal{N}$ pairs of lattice points satisfying $\mu-\mu'\perp\alpha$, since on a circle there are at most two chords with given length and direction. Thus, the sum for this range contains at most $\mathcal{N}$ terms:

$$\sum_{\substack{\mu\neq\mu'\\ \mu-\mu'\perp\alpha}}\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 = \sum_{\substack{\mu\neq\mu'\\ \mu-\mu'\perp\alpha}} L^2 \le L^2\cdot\mathcal{N}. \tag{A.1.6}$$

Given a summand

$$\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2$$

in the range $(\mu,\mu')\in A_\alpha$, we integrate and apply the triangle inequality:

$$\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 = \frac{|e^{2\pi iL\langle\mu-\mu',\alpha\rangle}-1|^2}{4\pi^2\langle\mu-\mu',\alpha\rangle^2} \le \frac{1}{\pi^2}\cdot\frac{1}{\langle\mu-\mu',\alpha\rangle^2}. \tag{A.1.7}$$

Also by the triangle inequality,

$$\left|\int_0^L e^{2\pi it\langle\mu-\mu',\alpha\rangle}dt\right|^2 \ll 1. \tag{A.1.8}$$

Combining (A.1.7) and (A.1.8),

$$\sum_{A_\alpha} \left| \int_0^L e^{2\pi i t \langle \mu - \mu', \alpha \rangle} dt \right|^2 \ll \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right). \tag{A.1.9}$$

The claim of the present lemma follows on replacing (A.1.5), (A.1.6) and (A.1.9) into (A.1.4). □

Proof of Proposition 3.3.2. We apply Proposition 3.2.1, Lemma A.1.1 and Lemma A.1.2:

$$\begin{aligned}
\mathrm{Var}(\mathcal{Z}) \ll m \cdot \mathfrak{R}_2(m) &\ll m \cdot \frac{1}{\mathcal{N}^2} \sum_{(\mu,\mu') \in \mathcal{E}^2} \left| \int_0^L e^{2\pi i t \langle \mu - \mu', \alpha \rangle} dt \right|^2 \\
&\ll \frac{m}{\mathcal{N}^2} \left[\mathcal{N} + \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right) \right] \\
&= \frac{m}{\mathcal{N}} + \frac{m}{\mathcal{N}^2} \cdot \sum_{A_\alpha} \min\left(1, \frac{1}{\langle \mu - \mu', \alpha \rangle^2}\right).
\end{aligned}$$

□

Appendix B

Proof of lemmas about lattice points on spheres

In this appendix, we prove Lemmas 4.4.5, 4.5.5 and 4.5.4.

Proof of Lemma 4.4.5. We write

$$S = T_2 \setminus T_1$$

where T_1 and T_2 are spherical caps of heights h_1, h_2, radii of bases k_1, k_2, and opening angles θ_1, θ_2 respectively; note that $h = h_2 - h_1$ and $k_2 = k$. Inserting $h_2 \ll R$ into the relation (4.4.1) for the cap T_2 yields

$$k_2 \asymp \sqrt{R}\sqrt{h_2}. \tag{B.1.1}$$

In case $h \asymp h_2$, we immediately have, by (B.1.1) and (4.4.3),

$$k\theta \leq k_2\theta_2 \ll \sqrt{R}\sqrt{h_2}\arcsin\left(\sqrt{h_2/2R}\right) \ll h_2 \asymp h,$$

which proves the lemma in this case.

The remaining case is $h = o(h_2)$: here we may write $h_2 = a + b$, $h_1 = a - b$, and $h = 2b$, with $0 \le b < a \le R$ and $b(R) = o(a(R))$ as $R \to \infty$. By (4.4.3),

$$\theta = \theta_2 - \theta_1 = 4\left[\arcsin\left(\sqrt{h_2/2R}\right) - \arcsin\left(\sqrt{h_1/2R}\right)\right].$$

By the expansion of arcsin around 0,

$$\begin{aligned}\theta &= 4\sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{4^n(2n+1)} \cdot \frac{(\sqrt{h_2})^{2n+1} - (\sqrt{h_1})^{2n+1}}{(\sqrt{2R})^{2n+1}} \\ &= 2\sqrt{2}\sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{8^n(2n+1)} \cdot \frac{(\sqrt{a+b})^{2n+1} - (\sqrt{a-b})^{2n+1}}{(\sqrt{R})^{2n+1}}.\end{aligned}$$

Multiplying and dividing by the quantity

$$(\sqrt{a+b})^{2n+1} + (\sqrt{a-b})^{2n+1}$$

we obtain

$$\begin{aligned}\theta &\ll \sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{8^n(2n+1)} \cdot \frac{(a+b)^{2n+1} - (a-b)^{2n+1}}{(aR)^{n+\frac{1}{2}}} \\ &\ll \sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{8^n(2n+1)} \cdot \frac{2\binom{2n+1}{1}a^{2n}b}{(aR)^{n+\frac{1}{2}}} = \frac{h}{\sqrt{R}\sqrt{a}}\sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{8^n} \cdot \left(\frac{a}{R}\right)^n. \end{aligned} \tag{B.1.2}$$

By (B.1.1) and (B.1.2), we have

$$k\theta \ll h\sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{8^n} \cdot \left(\frac{a}{R}\right)^n \le h\sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{8^n} = h\sqrt{2}.$$

$\square$

Proof of Lemma 4.5.5. Let $v, w \in \mathbb{R}^n$ be non-zero. By the triangle inequality:

$$\left\|\frac{v}{\|v\|}\|w\| - w\right\| = \left\|\frac{v}{\|v\|}\|w\| - v + v - w\right\| \le \left\|\frac{v}{\|v\|}\|w\| - v\right\| + \|v - w\|. \tag{B.1.3}$$

Applying the triangle inequality again,

$$\begin{aligned}\left\|\frac{v}{\|v\|}\|w\| - v\right\| &= \left\|\frac{v}{\|v\|}\|w\| - \frac{v}{\|v\|}\|v\|\right\| = \left\|\frac{v}{\|v\|}\right\| \cdot \big|\|w\| - \|v\|\big| \\ &= \big|\|w\| - \|v\|\big| \le \|v - w\|.\end{aligned} \tag{B.1.4}$$

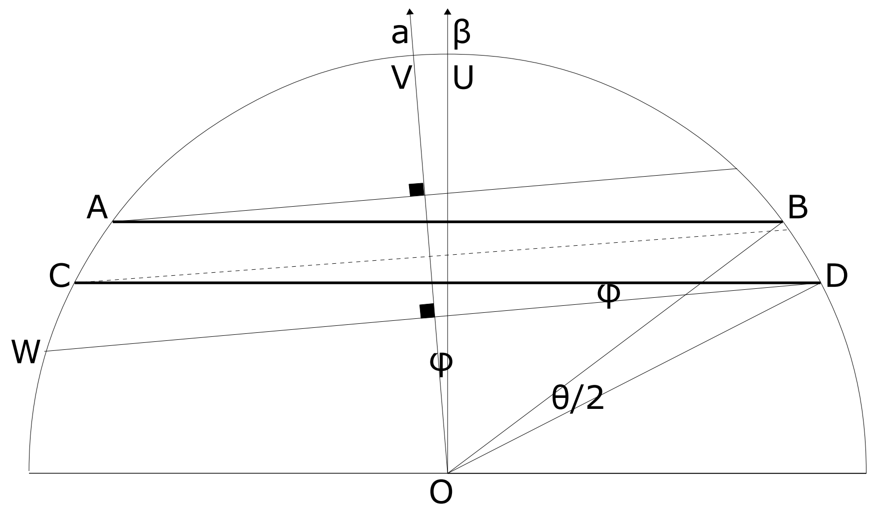

Figure B.1.1: Construction of the spherical segment S' (case 1); projection on the plane containing β and a.

Substituting (B.1.4) into (B.1.3) we get

$$\left\| \frac{v}{\|v\|}\|w\| - w \right\| \leq 2 \cdot \|v - w\| \Rightarrow \left\| \frac{v}{\|v\|} - \frac{w}{\|w\|} \right\| \leq 2\frac{\|v - w\|}{\|w\|}.$$

$\square$

Proof of Lemma 4.5.4. Fix a vector $a = (a_1, a_2, a_3) \in \mathbb{Z}^3$, and let φ be the angle between β and a (with a_1, a_2, a_3 parameters). Let $\mathcal{B}_1, \mathcal{B}_2$ be the bases of S (the latter being the larger), lying on the planes Π_1, Π_2 respectively. Denote O the origin, $U = R\beta \in R\mathcal{S}^2$ and $V = Ra/\|a\| \in R\mathcal{S}^2$ (see figure B.1.1).

With the same notation as Definition 4.4.4, call Γ the great circle through U and V. All arcs mentioned in this proof lie on the great circle Γ. Let $\{A, B\} := \mathcal{B}_1 \cap \Gamma$, $\{C, D\} := \mathcal{B}_2 \cap \Gamma$ (so that $\overline{AV} < \overline{BV}$ and $\overline{CV} < \overline{DV}$). As the opening angle of the spherical segment S is

$$\theta = \widehat{AOC} + \widehat{BOD} = 2 \cdot \widehat{AOC},$$

and the radius of the circle Γ is R, we have $\overset{\frown}{AC} = R \cdot \widehat{AOC} = R\theta/2$. There are three cases:

- <u>Case 1: $\overset{\frown}{UV} < \overset{\frown}{UA}$</u>.

  We shall consider a new spherical segment S', of direction $a/\|a\|$, and containing S; let S' be delimited by the following two planes: Π'_1 is defined to be orthogonal to a, and $A \in \Pi'_1$, while Π'_2 is defined to be orthogonal to a, and $D \in \Pi'_2$. Denote ψ and ψ' the number of lattice points in S and in S' respectively. Then we have

  $$\psi \leq \psi'. \tag{B.1.5}$$

  Since the direction of S' is the rational vector $a/\|a\|$, we may use Proposition 4.5.3:

  $$\psi' \leq \kappa(R) \cdot (1 + \|a\| \cdot h'), \tag{B.1.6}$$

  with $\kappa(R)$ as in Definition 1.3.1 and h' the height of S'. To estimate h', we start by considering S' as the disjoint union of two spherical segments S_1, S_2 as follows. The plane Π'_3 is defined to be orthogonal to a, with $C \in \Pi'_3$ (see figure B.1.1). Let S_1 be the segment delimited by Π'_1, Π'_3; let S_2 be the segment delimited by Π'_3, Π'_2. If we denote h_1 and h_2 the heights of S_1, S_2 respectively, then $h' = h_1 + h_2$. We have $h_1 < \overset{\frown}{AC} = \frac{R\theta}{2}$, and we will now show $h_2 < 2R\varphi$, hence

  $$h' = h_1 + h_2 \ll R(\theta + \varphi)$$

  which together with (B.1.5) and (B.1.6) yield (4.5.9). It remains to prove $h_2 < 2R\varphi$: denote W the point satisfying

  $$\{D, W\} = \Pi'_2 \cap \Gamma.$$

  Then $\overset{\frown}{CW}$ is an arc on Γ. We have $\widehat{CDW} = \widehat{UOV} = \varphi$, since $\overline{CD} \perp \overline{OU}$ and $\overline{DW} \perp \overline{OV}$. The height h_2 of S_2 is less than

  $$\overset{\frown}{CW} = R \cdot \widehat{COW} = 2R \cdot \widehat{CDW} = 2R\varphi.$$

- Case 2: $\widehat{UA} \leq \widehat{UV} \leq \widehat{UC}$.

  Denote Π' the plane orthogonal to a and containing D. The spherical cap T delimited by Π' has direction $a/\|a\|$ and contains S. Therefore, the number ψ of lattice points in S cannot exceed the number in T, which we will denote χ:

  $$\psi \leq \chi. \tag{B.1.7}$$

  Since the direction of T is the rational vector $a/\|a\|$, we may use [10, (2.13)]: as the opening angle of T is $\widehat{VOD}$, we have

  $$\chi \ll \kappa(R) \cdot \left[1 + R\|a\|(\widehat{VOD})^2\right]. \tag{B.1.8}$$

  We need to estimate $\widehat{VOD}$.

  $$\begin{aligned}\widehat{VOD} &= \widehat{VOU} + \widehat{UOD} = \widehat{VOU} + \widehat{UOC} = \widehat{VOU} + \widehat{VOU} + \widehat{VOC} \\ &\leq 2\widehat{VOU} + \widehat{AOC} = 2\varphi + \theta/2.\end{aligned}$$

  The latter inequality holds because we are assuming $\widehat{UA} \leq \widehat{UV} \leq \widehat{UC}$. By (B.1.7) and (B.1.8), we find

  $$\begin{aligned}\psi &\ll \kappa(R) \cdot \left[1 + R\|a\|(\widehat{VOD})^2\right] \leq \kappa(R) \cdot \left[1 + R\|a\|(2\varphi + \theta/2)^2\right] \\ &\ll \kappa(R) \cdot \left[1 + R\|a\|(\theta + \varphi)\right],\end{aligned}$$

  hence (4.5.9).

- Case 3: $\widehat{UC} < \widehat{UV}$.

  Consider the cap T of Case 2, of direction $a/\|a\|$ and containing S. We have (B.1.7), (B.1.8) and, since $\widehat{UC} < \widehat{UV}$,

  $$\widehat{VOD} = \widehat{VOU} + \widehat{UOD} = \widehat{VOU} + \widehat{UOC} < \widehat{VOU} + \widehat{VOU} = 2\varphi. \tag{B.1.9}$$

  By (B.1.7), (B.1.8) and (B.1.9),

  $$\begin{aligned}\psi &\ll \kappa(R) \cdot \left[1 + R\|a\|(\widehat{VOD})^2\right] < \kappa(R) \cdot \left[1 + R\|a\|(2\varphi)^2\right] \\ &\ll \kappa(R) \cdot \left[1 + R\|a\|(\theta + \varphi)\right],\end{aligned}$$

implying (4.5.9).

□

Appendix C

Gaussian integrals with perturbed covariance: Berry's method

In this appendix, we establish Lemma 5.5.8: following [5] and [47], we regard $\mathbb{E}[\|w_1\|\|w_2\|]$ (recall the notation in the statement of the lemma) as a function of the entries of the matrices X (5.4.9) and Y (5.4.10), and perform a Taylor expansion about $X = Y = 0$. We employ Berry's elegant method as opposed to computing the Taylor polynomial by brute force, which would result in a longer computation.

Lemma C.1.1. *Let $w_1, w_2 \in \mathbb{R}^3$, $(w_1, w_2) \sim N(0, \Omega)$ with $\Omega = I_6 + \begin{pmatrix} X & Y \\ Y & X \end{pmatrix}$. Then*

$$\mathbb{E}[\|w_1\|\|w_2\|] = \frac{1}{2\pi} \iint_{\mathbb{R}^2_+} (f(0,0) - f(t,0) - f(0,s) + f(t,s)) \frac{dtds}{(ts)^{3/2}} \tag{C.1.1}$$

with

$$f(t,s) = \frac{1}{\sqrt{\det\left(I_6 + J(t,s)\right)}}, \tag{C.1.2}$$

where

$$I_6 + J = \begin{pmatrix} (1+t)I_3 + tX & \sqrt{ts}Y \\ \sqrt{ts}Y & (1+s)I_3 + sX \end{pmatrix} \tag{C.1.3}$$

is a perturbation of the identity matrix I_6.

Proof. We begin with [5, (24)]:

$$\|w_i\| = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}_+} \left(1 - e^{-t\|w_i\|^2/2}\right) \frac{dt}{t^{3/2}}, \qquad i = 1, 2.$$

The LHS of (C.1.1) becomes

$$\begin{aligned} \mathbb{E}[\|w_1\|\|w_2\|] &= \frac{1}{2\pi} \iint_{\mathbb{R}_+^2} \mathbb{E}\left[(1 - e^{-t\|w_i\|^2/2})(1 - e^{-s\|w_i\|^2/2})\right] \frac{dtds}{(ts)^{3/2}} \\ &= \frac{1}{2\pi} \iint_{\mathbb{R}_+^2} \left(\mathbb{E}[1] + \mathbb{E}\left[-e^{-t\|w_1\|^2/2}\right] + \mathbb{E}\left[-e^{-s\|w_2\|^2/2}\right]\right. \\ &\qquad\qquad \left. + \mathbb{E}\left[e^{-(t\|w_1\|^2 + s\|w_2\|^2)/2}\right]\right) \frac{dtds}{(ts)^{3/2}}. \end{aligned}$$

Setting

$$f(t,s) = f_{X,Y}(t,s) := \mathbb{E}[\exp\{-(t\|w_1\|^2 + s\|w_2\|^2)/2\}],$$

it remains to show that $f(t,s)$ may be rewritten as in (C.1.2). By definition of expectation,

$$\begin{aligned} f(t,s) &= \int_{\mathbb{R}^3\times\mathbb{R}^3} \frac{1}{\sqrt{(2\pi)^6}} \cdot \frac{1}{\sqrt{\det\Omega}} \cdot \exp(-(t\|w_1\|^2 + s\|w_2\|^2)/2) \\ &\cdot \exp\left(-\frac{1}{2}\begin{pmatrix} w_1 & w_2 \end{pmatrix} \Omega^{-1} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\right) dw_1 dw_2 \\ &= \frac{1}{\sqrt{(2\pi)^6 \det\Omega}} \int_{\mathbb{R}^3\times\mathbb{R}^3} \exp\left(-\frac{1}{2}\begin{pmatrix} w_1 & w_2 \end{pmatrix}\left[\begin{pmatrix} tI_3 & 0 \\ 0 & sI_3 \end{pmatrix} + \Omega^{-1}\right]\begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\right) dw_1 dw_2 \\ &= \frac{1}{\sqrt{\det\Omega}} \cdot \sqrt{\det\left[\begin{pmatrix} tI_3 & 0 \\ 0 & sI_3 \end{pmatrix} + \Omega^{-1}\right]^{-1}} = \frac{1}{\sqrt{\det\left(I_6 + J(t,s)\right)}}, \end{aligned}$$

with $I_6 + J(t,s)$ as in (C.1.3). $\square$

We will need the following expansions for a square matrix P, as $P \to 0$ entry-wise:

$$(I+P)^{-1} = I - P + O(P^2) \tag{C.1.4}$$

and

$$(\det(I+P))^{-1/2} = 1 - \frac{1}{2}trP + \frac{1}{4}tr(P^2) + \frac{1}{8}(trP)^2 + O\left(\max_{i,j}(P^3)_{ij}\right). \tag{C.1.5}$$

Proof of Lemma 5.5.8. By Lemma C.1.1, we get the expression (C.1.1), and require the Taylor expansion of $f_{X,Y}(t,s) = \det(I_6+J)^{-1/2}$ around $X=Y=0$. By (C.1.3) and the formula for the determinant of a block matrix:

$$\det(I_6+J) = \det\left((1+t)I_3 + tX\right) \cdot \det\left[(1+s)I_3 + sX - \sqrt{ts}Y\left((1+t)I_3+tX\right)^{-1}\sqrt{ts}Y\right],$$

hence

$$\begin{aligned} &f_{X,Y}(t,s) = \det(I_6+J)^{-1/2} \\ &= \det((1+t)I_3+tX)^{-1/2} \cdot \det\left[(1+s)I_3 + sX - tsY((1+t)I_3+tX)^{-1}Y\right]^{-1/2}. \end{aligned} \tag{C.1.6}$$

Bearing in mind that I_3 and X are 3×3 matrices, we have

$$\det\left((1+t)I_3+tX\right) = (1+t)^3 \cdot \det\left(I_3 + \frac{t}{1+t}X\right)$$

and thus rewrite the first factor on the RHS of (C.1.6) as

$$\frac{1}{(1+t)^{3/2}}\det\left(I_3+\frac{t}{1+t}X\right)^{-1/2}. \tag{C.1.7}$$

Since

$$\begin{aligned} &\det\left[(1+s)I_3 + sX - tsY((1+t)I_3+tX)^{-1}Y\right] \\ &= \det\left\{(1+s)\left[I_3 + \frac{s}{1+s}X - \frac{ts}{(1+t)(1+s)}Y\left(I_3+\frac{t}{1+t}X\right)^{-1}Y\right]\right\}, \end{aligned}$$

the second factor on the RHS of (C.1.6) equals

$$\frac{1}{(1+s)^{3/2}} \det\left[I_3 + \frac{s}{1+s}X - \frac{ts}{(1+t)(1+s)}Y\left(I_3 + \frac{t}{1+t}X\right)^{-1} Y\right]^{-1/2};$$

applying (C.1.4) with $P = \frac{t}{1+t}X$, we further rewrite the second factor on the RHS of (C.1.6) as:

$$\begin{aligned}\frac{1}{(1+s)^{3/2}} \cdot \det\bigg[I + \frac{s}{1+s}X - \frac{ts}{(1+t)(1+s)}Y^2 \\ + \frac{t^2 s}{(1+t)^2(1+s)}YXY + O(YX^2Y)\bigg]^{-1/2}.\end{aligned} \tag{C.1.8}$$

Next, we apply (C.1.5) to both (C.1.7) and (C.1.8), with $P = \frac{t}{1+t}X$ and

$$P = \frac{s}{1+s}X - \frac{ts}{(1+t)(1+s)}Y^2 + \frac{t^2 s}{(1+t)^2(1+s)}YXY + O(YX^2Y)$$

respectively. The above computations on the two factors of (C.1.6) yield

$$\begin{aligned} f_{X,Y}(t,s) = &\frac{1}{(1+t)^{3/2}(1+s)^{3/2}} \cdot \bigg[1 - \frac{1}{2}\left(\frac{t}{1+t} + \frac{s}{1+s}\right) tr(X) \\ &+ \frac{1}{2} \cdot \frac{ts}{(1+t)(1+s)} tr(Y^2) - \frac{1}{2} \cdot \frac{ts}{(1+t)(1+s)}\left(\frac{t}{1+t} + \frac{s}{1+s}\right) tr(XY^2) \\ &+ \left(\frac{3}{8}\frac{t^2}{(1+t)^2} + \frac{3}{8}\frac{s^2}{(1+s)^2} + \frac{1}{4}\frac{ts}{(1+t)(1+s)}\right) tr(X^2) \\ &+ \frac{1}{4} \cdot \frac{t^2 s^2}{(1+t)^2(1+s)^2} tr(Y^4) + \frac{1}{8}\frac{t^2 s^2}{(1+t)^2(1+s)^2} tr(Y^2)^2 \\ &- \frac{1}{4} \cdot \frac{ts}{(1+t)(1+s)}\left(\frac{t}{1+t} + \frac{s}{1+s}\right) tr(X) tr(Y^2)\bigg] + O(tr(X^3) + tr(Y^6)), \end{aligned} \tag{C.1.9}$$

where we have used the assumption $\text{rank}(X) = 1$ so that $tr(X)^2 = tr(X^2)$. The integrand in (C.1.1) is

$$h_{X,Y}(t,s) := f(0,0) - f(t,0) - f(0,s) + f(t,s);$$

to compute the Taylor polynomial for h around $X = Y = 0$, first note that, except for the terms in $1, tr(X), tr(X^2)$, the various terms in the expansion of h are the same as those in the expansion of f: this is because each term in (C.1.9), save for those in $1, tr(X), tr(X^2)$, vanishes when $t = 0$ or $s = 0$. Next, we directly compute the terms in $1, tr(X), tr(X^2)$ of the expansion of h to be respectively

$$\left(1 - \frac{1}{(1+t)^{3/2}}\right) \cdot \left(1 - \frac{1}{(1+s)^{3/2}}\right),$$

$$\frac{1}{2}\left[\frac{t}{(1+t)^{5/2}}\left(1 - \frac{1}{(1+s)^{3/2}}\right) + \frac{s}{(1+s)^{5/2}}\left(1 - \frac{1}{(1+t)^{3/2}}\right)\right],$$

and

$$-\frac{3}{8}\frac{t^2}{(1+t)^{7/2}}\left(1 - \frac{1}{(1+s)^{3/2}}\right) - \frac{3}{8}\frac{s^2}{(1+s)^{7/2}}\left(1 - \frac{1}{(1+t)^{3/2}}\right) + \frac{1}{4}\frac{ts}{(1+t)^{5/2}(1+s)^{5/2}}.$$

To perform the integration

$$\mathbb{E}\left[\|w_1\|\|w_2\|\right] = \frac{1}{2\pi}\iint_{\mathbb{R}_+^2} h(t,s)\frac{dtds}{(ts)^{3/2}} \tag{C.1.10}$$

term-wise, we need to improve the error term $O(tr(X^3)+tr(Y^6))$ in the expansion of h so that it depends on t and s, as

$$\iint_{\mathbb{R}_+^2} \frac{dtds}{(ts)^{3/2}}$$

is divergent at the origin. To do this, we note that, for all X and Y, h vanishes when $t = 0$ or $s = 0$; hence, for $t, s \geq 0$, we may write

$$h_{X,Y}(t,s) = O_{X,Y}(ts).$$

We may then improve the error term in the expansion of h to

$$O\left(\min(t,1) \cdot \min(s,1) \cdot (tr(X^3) + tr(Y^6))\right).$$

Therefore,

$$
\begin{aligned}
h^{X,Y}(t,s) = & \left(1 - \frac{1}{(1+t)^{3/2}}\right) \cdot \left(1 - \frac{1}{(1+s)^{3/2}}\right) \\
& + \frac{1}{2}\left[\frac{t}{(1+t)^{5/2}}\left(1 - \frac{1}{(1+s)^{3/2}}\right) + \frac{s}{(1+s)^{5/2}}\left(1 - \frac{1}{(1+t)^{3/2}}\right)\right] tr(X) \\
& + \frac{1}{2}\frac{t}{(1+t)^{5/2}}\frac{s}{(1+s)^{5/2}} tr(Y^2) - \frac{1}{2}\left(\frac{t^2}{(1+t)^{7/2}}\frac{s}{(1+s)^{5/2}}\right. \\
& \left. + \frac{t}{(1+t)^{5/2}}\frac{s^2}{(1+s)^{7/2}}\right) tr(XY^2) + \left[-\frac{3}{8}\frac{t^2}{(1+t)^{7/2}}\left(1 - \frac{1}{(1+s)^{3/2}}\right)\right. \\
& \left. - \frac{3}{8}\frac{s^2}{(1+s)^{7/2}}\left(1 - \frac{1}{(1+t)^{3/2}}\right) + \frac{1}{4}\frac{ts}{(1+t)^{5/2}(1+s)^{5/2}}\right] tr(X^2) \\
& + \frac{1}{4}\frac{t^2s^2}{(1+t)^{7/2}(1+s)^{7/2}} tr(Y^4) + \frac{1}{8}\frac{t^2s^2}{(1+t)^{7/2}(1+s)^{7/2}} tr(Y^2)^2 \\
& - \frac{1}{4}\left(\frac{ts^2}{(1+t)^{5/2}(1+s)^{7/2}} + \frac{t^2s}{(1+t)^{7/2}(1+s)^{5/2}}\right) tr(X)tr(Y^2) \\
& + O\left(\min(t,1) \cdot \min(s,1) \cdot (tr(X^3) + tr(Y^6))\right).
\end{aligned}
\tag{C.1.11}
$$

Lastly, we insert (C.1.11) into (C.1.1), and compute the integrals

$$
\int_0^\infty \left(1 - \frac{1}{(1+t)^{3/2}}\right)\frac{dt}{t^{3/2}} = 4, \qquad \int_0^\infty \frac{dt}{(1+t)^{5/2}\sqrt{t}} = \frac{4}{3},
$$

$$
\int_0^\infty \frac{\sqrt{t}\ dt}{(1+t)^{7/2}} = \frac{4}{15}, \qquad \int_0^\infty \min(t,1)\frac{dt}{t^{3/2}} = 4,
$$

to obtain the statement of the present lemma. □

Bibliography

[1] Robert J. Adler and Jonathan E. Taylor. *Random fields and geometry*. Springer Monographs in Mathematics. Springer, New York, 2007.

[2] Jean-Marc Azaïs and Mario Wschebor. *Level sets and extrema of random processes and fields*. John Wiley & Sons, Inc., Hoboken, NJ, 2009.

[3] Yu K Belyaev. On the number of intersections of a level by a gaussian stochastic process. i. *Theory of Probability & Its Applications*, 11(1):120–128, 1966.

[4] Jacques Benatar and Riccardo W. Maffucci. Random waves on $\mathbb{T}^3$: Nodal area variance and lattice point correlations. *International Mathematics Research Notices*, to appear.

[5] Michael V Berry. Statistics of nodal lines and points in chaotic quantum billiards: perimeter corrections, fluctuations, curvature. *Journal of Physics A: Mathematical and General*, 35(13):3025, 2002.

[6] Enrico Bombieri and Jean Bourgain. A problem on sums of two squares. *International Mathematics Research Notices*, 2015(11):3343–3407, 2015.

[7] Jean Bourgain. On toral eigenfunctions and the random wave model. *Israel Journal of Mathematics*, 201(2):611–630, 2014.

[8] Jean Bourgain and Zeév Rudnick. On the geometry of the nodal lines of eigenfunctions of the two-dimensional torus. *Ann. Henri Poincaré*, 12(6):1027–1053, 2011.

[9] Jean Bourgain and Zeév Rudnick. On the nodal sets of toral eigenfunctions. *Invent. Math.*, 185(1):199–237, 2011.

[10] Jean Bourgain and Zeév Rudnick. Restriction of toral eigenfunctions to hypersurfaces and nodal sets. *Geom. Funct. Anal.*, 22(4):878–937, 2012.

[11] Jean Bourgain and Zeév Rudnick. Nodal intersections and L^p restriction theorems on the torus. *Israel Journal of Mathematics*, 207(1):479–505, 2015.

[12] Jean Bourgain, Peter Sarnak, and Zeév Rudnick. Local statistics of lattice points on the sphere. *Modern Trends in Constructive Function Theory, Contemp. Math*, 661:269–282, 2012.

[13] Jean Bourgain and Nigel Watt. Mean square of zeta function, circle problem and divisor problem revisited. *arXiv preprint arXiv:1709.04340*, 2017.

[14] Jochen Brüning. Über knoten von eigenfunktionen des laplace-beltrami-operators. *Mathematische Zeitschrift*, 158(1):15–21, 1978.

[15] Jochen Brüning and Dieter Gromes. Über die länge der knotenlinien schwingender membranen. *Mathematische Zeitschrift*, 124(1):79–82, 1972.

[16] Yaiza Canzani and John A Toth. Nodal sets of Schrödinger eigenfunctions in forbidden regions. *Annales Henri Poincaré*, 17(11):3063–3087, 2016.

[17] J. W. S. Cassels. *An introduction to the geometry of numbers.* Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[18] Shiu-Yuen Cheng. Eigenfunctions and nodal sets. *Commentarii Mathematici Helvetici*, 51(1):43–55, 1976.

[19] J. Cilleruelo and A. Córdoba. Trigonometric polynomials and lattice points. *Proc. Amer. Math. Soc.*, 115(4):899–905, 1992.

[20] Javier Cilleruelo. The distribution of the lattice points on circles. *J. Number Theory*, 43(2):198–202, 1993.

[21] Javier Cilleruelo and Andrew Granville. Lattice points on circles, squares in arithmetic progressions and sumsets of squares. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 241–262. Amer. Math. Soc., Providence, RI, 2007.

[22] Javier Cilleruelo and Andrew Granville. Close lattice points on circles. *Canad. J. Math.*, 61(6):1214–1238, 2009.

[23] Harald Cramér and M. R. Leadbetter. *Stationary and related stochastic processes. Sample function properties and their applications*. John Wiley & Sons, Inc., New York-London-Sydney, 1967.

[24] Harold Davenport. *The higher arithmetic: an introduction to the theory of numbers*. Cambridge University Press, 1999.

[25] Manfredo P. do Carmo. *Differential geometry of curves and surfaces*. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1976. Translated from the Portuguese.

[26] Harold Donnelly and Charles Fefferman. Nodal sets of eigenfunctions on riemannian manifolds. *Inventiones mathematicae*, 93(1):161–183, 1988.

[27] William Duke. Hyperbolic distribution problems and half-integral weight maass forms. *Inventiones mathematicae*, 92(1):73–90, 1988.

[28] William Duke and Rainer Schulze-Pillot. Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids. *Inventiones Mathematicae*, 99(1):49–57, 1990.

[29] Layan El-Hajj and John A Toth. Intersection bounds for nodal sets of planar Neumann eigenfunctions with interior analytic curves. *Journal of Differential Geometry*, 100(1):1–53, 2015.

[30] Paul Erdös and Richard Roxby Hall. On the angular distribution of gaussian integers with fixed norm. *Discrete mathematics*, 200(1-3):87–94, 1999.

[31] Laura Fainsilber, Pär Kurlberg, and Bernt Wennberg. Lattice points on circles and discrete velocity models for the Boltzmann equation. *SIAM J. Math. Anal.*, 37(6):1903–1922 (electronic), 2006.

[32] Herbert Federer. *Geometric measure theory*. Springer-Verlag New York Inc., New York, 1969.

[33] Jacob Fox, János Pach, Adam Sheffer, Andrew Suk, and Joshua Zahl. A semi-algebraic version of Zarankiewicz's problem. *arXiv preprint arXiv:1407.5705*, 2014.

[34] Amit Ghosh, Andre Reznikov, and Peter Sarnak. Nodal domains of Maass forms I. *Geom. Funct. Anal.*, 23(5):1515–1568, 2013.

[35] Elena Petrovna Golubeva and Oleg Mstislavovich Fomenko. Asymptotic distribution of integral points on the three-dimensional sphere. *Zapiski Nauchnykh Seminarov POMI*, 160:54–71, 1987.

[36] Andrew Granville and Igor Wigman. Planck-scale mass equidistribution of toral Laplace eigenfunctions. *Comm. Math. Phys.*, 355(2):767–802, 2017.

[37] Emil Grosswald. *Representations of integers as sums of squares*. Springer Science & Business Media, 2012.

[38] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press, Oxford University Press, New York, fifth edition, 1979.

[39] Godfrey Harold Hardy. *On the expression of a number as the sum of two squares*, volume 46. 1915.

[40] Lars Hörmander. The spectral function of an elliptic operator. *Acta mathematica*, 121(1):193–218, 1968.

[41] Martin N Huxley. Exponential sums and lattice points iii. *Proceedings of the London Mathematical Society*, 87(3):591–609, 2003.

[42] Victor Ivrii. 100 years of Weyl's law. *Bulletin of Mathematical Sciences*, 6(3):379–452, 2016.

[43] Henryk Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Inventiones mathematicae*, 87(2):385–401, 1987.

[44] Henryk Iwaniec. *Topics in classical automorphic forms*, volume 17. American Mathematical Soc., 1997.

[45] Vojtěch Jarník. Über die Gitterpunkte auf konvexen Kurven. *Math. Z.*, 24(1):500–518, 1926.

[46] Yitzhak Katznelson. *An introduction to harmonic analysis*. Cambridge University Press, 2004.

[47] Manjunath Krishnapur, Pär Kurlberg, and Igor Wigman. Nodal length fluctuations for arithmetic random waves. *Ann. of Math. (2)*, 177(2):699–737, 2013.

[48] Lauwerens Kuipers and Harald Niederreiter. *Uniform distribution of sequences*. Courier Corporation, 2012.

[49] Pär Kurlberg and Igor Wigman. On probability measures arising from lattice points on circles. *Mathematische Annalen*, 367(3-4):1057–1098, 2017.

[50] Edmund Landau. *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*. Archiv der Mathematik und Physik, Ser. III, Bd. XIII. 1908.

[51] Alexander Logunov. Nodal sets of Laplace eigenfunctions: proof of Nadirashvili's conjecture and of the lower bound in Yau's conjecture. *arXiv preprint arXiv:1605.02589*, 2016.

[52] Riccardo W. Maffucci. Nodal intersections for random waves against a segment on the 3-dimensional torus. *Journal of Functional Analysis*, 272(12):5218–5254, 2017.

[53] Riccardo W. Maffucci. Nodal intersections of random eigenfunctions against a segment on the 2-dimensional torus. *Monatshefte für Mathematik*, 183(2):311–328, 2017.

[54] Ferenc Oravecz, Zeév Rudnick, and Igor Wigman. The Leray measure of nodal sets for random eigenfunctions on the torus. *Annales de l'Institut Fourier*, 58(1):299–335, 2008.

[55] Andrzej Palczewski, Jacques Schneider, and Alexandre V. Bobylev. A consistency result for a discrete-velocity model of the Boltzmann equation. *SIAM J. Numer. Anal.*, 34(5):1865–1883, 1997.

[56] Gordon Pall. Quaternions and sums of three squares. *American Journal of Mathematics*, 64(1):503–513, 1942.

[57] Yiannis Petridis and John A Toth. The remainder in Weyl's law for random two-dimensional flat tori. *Geometric and Functional Analysis*, 12(4):756–775, 2002.

[58] Christian Pommerenke. Über die gleichverteilung von gitterpunkten auf m-dimensionalen ellipsoiden. *Acta arithmetica*, 5(2):227–257, 1959.

[59] Maurizia Rossi and Igor Wigman. Asymptotic distribution of nodal intersections for arithmetic random waves. *arXiv preprint arXiv:1702.05179*, 2017.

[60] Zeév Rudnick and Igor Wigman. On the volume of nodal sets for eigenfunctions of the Laplacian on the torus. *Ann. Henri Poincaré*, 9(1):109–130, 2008.

[61] Zeév Rudnick and Igor Wigman. Nodal intersections for random eigenfunctions on the torus. *Amer. J. Math.*, 138(6):1605–1644, 2016.

[62] Zeév Rudnick, Igor Wigman, and Nadav Yesha. Nodal intersections for random waves on the 3-dimensional torus. *Ann. Inst. Fourier (Grenoble)*, 66(6):2455–2484, 2016.

[63] Yu Safarov and D Vassilev. *The asymptotic distribution of eigenvalues of partial differential operators*, volume 155. American Mathematical Soc., 1997.

[64] Peter Sarnak. *Some applications of modular forms*, volume 99. Cambridge University Press, 1990.

[65] Wolfgang M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[66] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[67] John A. Toth and Steve Zelditch. Counting nodal lines which touch the boundary of an analytic domain. *J. Differential Geom.*, 81(3):649–686, 2009.

[68] Samuel S. Wagstaff, Jr. The Schnirelmann density of the sums of three squares. *Proc. Amer. Math. Soc.*, 52:1–7, 1975.

[69] Igor Wigman. Private communication.

[70] Igor Wigman. Fluctuations of the nodal length of random spherical harmonics. *Communications in Mathematical Physics*, 298(3):787–831, 2010.

[71] Shing-Tung Yau. Survey on partial differential equations in differential geometry. *Ann. Math. Studies*, 102:3–70, 1982.

[72] Shing-Tung Yau. Open problems in geometry. In *Proc. Symp. Pure Math*, volume 54, pages 1–28, 1993.

[73] Nadav Yesha. Eigenfunction statistics for a point scatterer on a three-dimensional torus. *Annales Henri Poincaré*, 14(7):1801–1836, 2013.

[74] A. Zygmund. On Fourier coefficients and transforms of functions of two variables. *Studia Math.*, 50:189–201, 1974.